PROJEKTVERTRAG

[redacted]

zwischen

virtual7 GmbH
Amalienbadstraße 41d
76227 Karlsruhe

– nachfolgend „virtual7“ oder „Subunternehmerin“ genannt –

und der

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main

– nachfolgend „TSI“ genannt,

TSI und virtual7 jeweils auch „Partei“ oder zusammen die „Parteien“ genannt –

Anlagen

1. Kundenspezifische Regelungen
    a. Anhang 1 (Anforderungen an die Informationssicherheit der BWI)
    b. Anhang 2 (Vereinbarung zur Auftragsverarbeitung)
    c. Anhang 3 (Vereinbarung zur weiteren Auftragsverarbeitung)
    d. Anhang 4 (VS-Merkblatt)
    e. Anhang 5a (Empfehlung zur Korruptionsprävention)
    f. Anhang 5b (Richtlinie zur Korruptionsprävention)
    g. Anhang 5c (Umsetzung der Richtlinie zur Korruptionsprävention)

h. Anhang 6 (Zentrale Dienstvorschrift zur Annahme von Zuwendungen)

i. Anhang 7 (Zusätzliche Vertragsbedingungen BmVG)

j. Anhang 8 (Verpflichtung nichtbeamteter Personen)

k. Anhang 9 (Open Source Software)

2. Vergütung
3. Bestellprozess
4. Leistungsbeschreibung des Kunden: Anl. 1 zum RV_Leistungsbeschreibung_pCloudBw
5. Anhang zur Leistungsbeschreibung: Anhang zur LB_PM@BWI4ext_pCloudBw

   5.1 „Software Engeneering Framework 2024“
6. Preisblatt
7. Supplier Code of Conduct Version 2024
8. EB ICT-Services Version 2024

Die T-Systems International (TSI) wird mit dem Kunden BWI („Kunde“) einen Rahmenvertrag über den Bezug von Konzeptions- und Entwicklungsleistungen für die „Strategische Partnerschaft pCloudBw“ („Rahmenvertrag“) abschließen. Die T-Systems ist dabei für die Steuerung der Subunternehmer unter diesem Vertrag verantwortlich.

TSI wird die Subunternehmerin mit der Leistungserbringung beauftragen, wobei die rechtsverbindliche Auftragserteilung erst mit einem gesonderten Einkaufsvertrag, d. h. mit einer Bestellung der DTAG, welche auf den Bedingungen dieser Vereinbarung basiert, erfolgt. Sollte TSI von einer Bestellung absehen, gleich aus welchen Gründen oder Umständen, bestehen keine Ansprüche der Subunternehmerin gegen TSI, mit Ausnahme für vorsätzlich schädigendes Verhalten der TSI.

Für die gemeinsame Zusammenarbeit unter dem Rahmenvertrag bzw. den daraus resultierenden Einzelaufträgen vereinbaren die Parteien folgendes:

(1) Die Subunternehmerin erklärt, dass ihr die relevanten Vergabeunterlagen bekannt sind und dass sie auf dieser Grundlage TSI die von ihr als Subunternehmerin zu erbringenden Leistungen anbietet.

Die relevanten rechtlichen, kommerziellen und technischen Konditionen des Rahmenvertrages und seiner Anlagen sind diesem Projektvertrag als Anlagen und Anhänge beigefügt. Die Subunternehmerin bestätigt hiermit ausdrücklich, dass sie die an die Subunternehmerin zu stellenden Verpflichtungen und Anforderungen in dem Umfang akzeptiert, wie sie nach diesem Projektvertrag und seinen Anlagen und Anhängen gestellt werden. Dazu zählen insbesondere die

Nutzungs- und Verwertungsrechte, die Audit- und Zutrittsrechte, die datenschutzrechtlichen Vorgaben und die Vertraulichkeitsbestimmungen. Diese Dokumente gelten für die Leistungserbringung gegenüber TSI. Abweichende Allgemeine Geschäftsbedingungen der Subunternehmerin, werden nicht Vertragsbestandteil.

Die Subunternehmerin wird die TSI von allen eventuellen Ansprüchen des Kunden oder Dritten insoweit freistellen, als die Leistungen aus dem Vertragsverhältnis mit dem Kunden oder Dritten in den Verantwortungsbereich der Subunternehmerin bzw. von ihr mit der Leistungserbringung beauftragten Dritten fallen. Dies gilt insbesondere für Schadensersatz- und Aufwendungsersatzansprüche sowie für Ansprüche aus Gewährleistung (Mängelansprüche), Verzug und Nacherfüllung bzw. Schlechterfüllung, Freistellungsverpflichtungen, Vertragsstrafen. Die vorstehenden Sätze gelten entsprechend auch für eigene Ansprüche der TSI.

(2) Eine Unterbeauftragung durch die Subunternehmerin bedarf der vorherigen schriftlichen Zustimmung von TSI (die wiederum vorher die schriftliche Zustimmung von dem Kunden einholen muss). Unterauftragnehmer sind von der Subunternehmerin auf die Einhaltung der für den Kunden geltenden Bestimmungen gemäß dieses Projektvertrages und seiner Anlagen sowie des jeweiligen Einzelauftrags zu verpflichten, insbesondere in Bezug auf Entsorgungs- und Exportvorschriften, die Informationssicherheit, die Vertraulichkeit, die Behandlung von Verschlusssachen, den Datenschutz und den Verhaltenskodex. Im Übrigen gelten die Regelungen von Ziffer 15 der EB ICT-Services (Anlage 8).

(3) Die Vergütung der Subunternehmerin erfolgt gemäß den Regelungen der Anlage 2.

(4) Der Bestellprozess erfolgt gemäß den Regelungen der Anlage 3.

(5) Sollten nach Abschluss dieses Projektvertrages Leistungsänderungen oder zusätzliche vertragliche Verpflichtungen mit dem Kunden verhandelt werden, so wird TSI diese der Subunternehmerin unverzüglich übermitteln und sind durch diese zu bestätigen. Den sich aus diesen Änderungen ergebenden Anpassungsbedarf dieses Projektvertrages werden die Parteien jeweils in Form von Nachträgen zu diesem Projektvertrag regeln.

(6) TSI ist verpflichtet, die Subunternehmerin bei der Geltendmachung von Mitwirkungspflichten gegenüber dem Kunden zu unterstützen.

(7) Die im Rahmen der Zusammenarbeit ausgetauschten Informationen und Daten sind vertraulich und dürfen nur für die Zwecke dieses Vertrages verwendet werden. Die Parteien verpflichten sich, diese Informationen weder Dritten offen zu legen noch zuzulassen, dass diese offengelegt oder vervielfältigt werden. Diese Verpflichtung gilt nicht für solche Informationen, die ohne Bruch dieser Vereinbarung allgemein bekannt sind oder werden, die nachweislich unabhängig erarbeitet oder von Dritten rechtmäßig, ohne Verpflichtung zur Geheimhaltung, erlangt wurden oder zum Zeitpunkt der Offenbarung bereits im Besitz der empfangenden Partei waren. Als Dritte gelten nicht konzernverbundene Unternehmen sowie weitere potenzielle Subunternehmer der TSI. Die Verpflichtung der Geheimhaltung gilt auch nach Beendigung der Zusammenarbeit fort.

(8) Die Laufzeit dieses Projektvertrages beginnt mit dem Datum der letzten Vertragsunterschrift durch die Parteien in Kraft. Der Projektvertrag wird – vorbehaltlich einer vorzeitigen Beendigung nach Maßgabe der nachfolgenden Bestimmungen – für eine feste Laufzeit von sieben (7) Jahren abgeschlossen (nachfolgend „Grundlaufzeit“ genannt). TSI ist berechtigt, den Projektvertrag bis zum zweiten Monat vor dem Ende seiner jeweiligen Laufzeit durch einseitige Erklärung 3-malig in Textform um jeweils ein (1) Jahr zu verlängern (nachfolgend „Optionszeitraum“ genannt). Die maximale Gesamtlaufzeit des Projektvertrages setzt sich zusammen aus der Grundlaufzeit und dem Optionszeitraum.

TSI ist jederzeit berechtigt, den Projektvertrag mit einer Frist von elf (11) Monaten zum Kalenderjahresende ganz oder teilweise zu kündigen. Während der Laufzeit dieses Projektvertrages abgeschlossene Einzelaufträge bleiben von einer Beendigung des

Projektvertrages unberührt. Bis zur Beendigung des Einzelauftrags gelten die Regelungen des Projektvertrags für den jeweiligen Einzelauftrag fort. Vorstehendes gilt nicht, sofern TSI einen Einzelauftrag außerordentlich gekündigt hat.

Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt. Soweit der Rahmenvertrag zwischen dem Kunden und TSI gleich aus welchem Grund endet, ist TSI gegenüber der Subunternehmerin zur Kündigung dieses Vertrages zum selben Beendigungszeitpunkt berechtigt.

(9) Änderungen oder Ergänzungen dieser Vereinbarung bedürfen der Schriftform und sind von beiden Parteien zu unterzeichnen.

(10) Die folgenden Dokumente gelten in der dargestellten Reihenfolge:

1. Bestellung
2. der Projektvertrag inklusive sämtlicher Anlagen und Anhänge
3. EB ICT-Services

Signatures

Number of pages (including this one): 5

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

Eigenerklärung zur Umsetzung der Sanktionsverordnung

Bietergemeinschaften: Die Eigenerklärung ist von jedem Mitglied der Bietergemeinschaft abzugeben.

Der Unterauftragnehmer:

virtual7 GmbH

Name des Unterauftragnehmers

Die nachfolgende Erklärung gebe/n ich/wir verbindlich ab (ggf. zugleich in Vertretung für die lt. Angebot Vertretenen auch für diese):

1. Der **Unterauftragnehmer** gehört nicht zu den

in **Artikel 5 k)** Absatz 1 der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren,

genannten Personen oder Unternehmen, die einen Bezug zu Russland im Sinne der Vorschrift aufweisen,

a) **durch die russische Staatsangehörigkeit des Bieters oder die Niederlassung des Bieters in Russland,**
b) **durch die Beteiligung einer natürlichen Person oder eines Unternehmens, auf die eines der Kriterien nach Buchstabe a zutrifft, am Bieter über das Halten von Anteilen im Umfang von mehr als 50%,**
c) **durch das Handeln der Bieter im Namen oder auf Anweisung von Personen oder Unternehmen, auf die die Kriterien der Buchstaben a und/oder b zutrifft.**

2. Die am Auftrag als **Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Zusammenhang mit der Erbringung des Eignungsnachweises in Anspruch genommen werden**, beteiligten Unternehmen, auf die mehr als 10 % des Auftragswerts entfällt, gehören ebenfalls nicht zu dem in der Vorschrift genannten Personenkreis mit einem Bezug zu Russland im Sinne der Vorschrift.

3. Es wird bestätigt und sichergestellt, dass auch während der Vertragslaufzeit keine als **Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Zusammenhang mit der Erbringung des Eignungsnachweises in Anspruch genommen werden**, beteiligten Unternehmen eingesetzt werden, auf die mehr als 10 % des Auftragswerts entfällt.

[redacted]

Artikel 5k der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 lautet wie folgt:

(1) Es ist verboten, öffentliche Aufträge oder Konzessionen, die in den Anwendungsbereich der Richtlinien über die öffentliche Auftragsvergabe sowie unter Artikel 10 Absatz 1, Absatz 3, Absatz 6 Buchstaben a bis e, Absatz 8, Absatz 9 und Absatz 10 und die Artikel 11, 12, 13 und 14 der Richtlinie 2014/23/EU, unter die Artikel 7 und 8, Artikel 10 Buchstaben b bis f und h bis j der Richtlinie 2014/24/EU, unter Artikel 18, Artikel 21 Buchstaben b bis e und g bis i, Artikel 29 und Artikel 30 der Richtlinie 2014/25/EU und unter Artikel 13 Buchstaben a bis d, f bis h und j der Richtlinie 2009/81/EG fallen, an folgende Personen, Organisationen oder Einrichtungen zu vergeben bzw. Verträge mit solchen Personen, Organisationen oder Einrichtungen weiterhin zu erfüllen:

a) russische Staatsangehörige oder in Russland niedergelassene natürliche oder juristische Personen, Organisationen oder Einrichtungen,

b) juristische Personen, Organisationen oder Einrichtungen, deren Anteile zu über 50 % unmittelbar oder mittelbar von einer der unter Buchstabe a genannten Organisationen gehalten werden, oder

c) natürliche oder juristische Personen, Organisationen oder Einrichtungen, die im Namen oder auf Anweisung einer der unter Buchstabe a oder b genannten Organisationen handeln,

auch solche, auf die mehr als 10 % des Auftragswerts entfällt, Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Sinne der Richtlinien über die öffentliche Auftragsvergabe in Anspruch genommen werden.

(2) Abweichend von Absatz 1 können die zuständigen Behörden die Vergabe oder die Fortsetzung der Erfüllung von Verträgen genehmigen, die bestimmt sind für

a) den Betrieb ziviler nuklearer Kapazitäten, ihre Instandhaltung, ihre Stilllegung, die Entsorgung ihrer radioaktiven Abfälle, ihre Versorgung mit und die Wiederaufbereitung von Brennelementen und die Weiterführung der Planung, des Baus und die Abnahmetests für die Indienststellung ziviler Atomanlagen und ihre Sicherheit sowie die Lieferung von Ausgangsstoffen zur Herstellung medizinischer Radioisotope und ähnlicher medizinischer Anwendungen, kritischer Technologien zur radiologischen Umweltüberwachung sowie für die zivile nukleare Zusammenarbeit, insbesondere im Bereich Forschung und Entwicklung,

b) die zwischenstaatliche Zusammenarbeit bei Raumfahrtprogrammen,

c) die Bereitstellung unbedingt notwendiger Güter oder Dienstleistungen, wenn sie ausschließlich oder nur in ausreichender Menge von den in Absatz 1 genannten Personen bereitgestellt werden können,

d) die Tätigkeit der diplomatischen und konsularischen Vertretungen der Union und der Mitgliedstaaten in Russland, einschließlich Delegationen, Botschaften und Missionen, oder internationaler Organisationen in Russland, die nach dem Völkerrecht Immunität genießen.

e) den Kauf, die Einfuhr oder die Beförderung von Erdgas und Erdöl, einschließlich raffinierter Erdölerzeugnisse, sowie von Titan, Aluminium, Kupfer, Nickel, Palladium und Eisenerz aus oder durch Russland in die Union, oder

f) den Kauf, die Einfuhr oder die Beförderung von Kohle und anderen festen fossile Brennstoffen, die in Anhang XXII aufgeführt sind, bis 10. August 2022.

(3) Der betreffende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten und die Kommission über jede nach diesem Artikel erteilte Genehmigung innerhalb von zwei Wochen nach deren Erteilung.

(4) Die Verbote gemäß Absatz 1 gelten nicht für die Erfüllung — bis zum 10. Oktober 2022 — von Verträgen, die vor dem 9. April 2022 geschlossen wurden.

Signatures

Number of pages (including this one): 3

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

Anlage 1 – Kundenspezifische Regelungen

Bei den nachfolgenden Regelungen handelt es sich um Regelungen aus dem Rahmenvertrag, die auch für die Subunternehmerin Anwendung finden. „Auftraggeber“ ist im Folgenden die T-Systems, „Auftragnehmer“ die Subunternehmerin.

1 Rechtseinräumung und vorbestehende Werke

1.1

Der Auftragnehmer ist verpflichtet, alle geistigen Eigentumsrechte, die an den auf Grundlage dieses Projektvertrages speziell für den Kunden erstellten schutzfähigen und nicht schutzrechtsfähigen Werken oder sonstigen Arbeitsergebnissen (nachfolgend gemeinsam „Arbeitsergebnisse” genannt) entstehen, an den Kunden zu übertragen. Diese übertragenen Rechte stehen dem Kunden ausschließlich, inhaltlich, zeitlich und räumlich unbeschränkt, unwiderruflich und unkündbar zu und sind unterlizenzierbar und übertragbar.

Der Auftragnehmer informiert den Auftraggeber, falls und soweit er beabsichtigt, ein Arbeitsergebnis zukünftig auch gegenüber anderen Kunden zu vertreiben oder entwickelte Arbeitsergebnisse in seine Produkte aufnehmen möchte. Sofern der Auftraggeber einer Weiterverwendung durch den Auftragnehmer zustimmt, stimmen sich die Parteien über die konkrete Ausgestaltung ab und vereinbaren diese in einem Nachtrag zu diesem Projektvertrag.

1.2

Der Auftragnehmer hat zudem bei Arbeitsergebnissen in Form von Software (z.B. Individualsoftware oder angepasste (customizierte) Standardsoftware) dem Kunden nach erfolgter Abnahme der Software deren Quellcode in strukturierter und pflegefähiger Form inklusive einer den Quellcode ausführlich beschreibenden und erläuternden Programmdokumentation in deutscher oder englischer Sprache sowie der Nennung der Namen und Versionen der Entwicklungswerkzeuge bereitzustellen, wobei die Bereitstellung entweder auf einem marktüblichen Datenträger an die von dem Auftraggeber angegebene Lieferadresse oder durch eine Bereitstellung zum Abruf über das Internet (Download) erfolgt.

1.3

Sofern eine Übertragung von Rechten nach Ziffer 1.1 dieser Anlage 1 aus rechtlichen Gründen nicht möglich ist, räumt der Auftragnehmer dem Kunden an den Arbeitsergebnissen ausschließliche, unwiderrufliche, inhaltlich, räumlich und zeitlich unbeschränkte, unterlizenzierbare und übertragbare Nutzungs- und Verwertungsrechte ein. Die vorstehende Rechtseinräumung umfasst insbesondere auch das Recht zur Vervielfältigung, zur Verbreitung, zur Ausstellung, zur Bearbeitung oder anderen Umgestaltungen und zur öffentlichen Wiedergabe. Soweit es sich bei den Arbeitsergebnissen um Software handelt, umfasst die Rechtseinräumung insbesondere folgende Rechte:

- die dauerhafte oder vorübergehende Vervielfältigung des Arbeitsergebnisses, ganz oder teilweise, mit jedem Mittel und in jeder Form, insbesondere anlässlich des Ladens, Anzeigens, Ablaufen Lassens, Übertragens oder Speicherns des Arbeitsergebnisses
- die Übersetzung, die Bearbeitung, das Arrangement und andere Umarbeitungen des Arbeitsergebnisses, einschließlich des Rechts, die erzielten Ergebnisse zu vervielfältigen

- das Recht, das Original oder Vervielfältigungsstücke des Arbeitsergebnisses in jeder Form zu verbreiten, einschließlich des Rechts, das Arbeitsergebnis zu vermieten
- das Recht, das Arbeitsergebnis drahtgebunden oder drahtlos öffentlich wiederzugeben, einschließlich des Rechts zur öffentlichen Zugänglichmachung in der Weise, dass es Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich ist
- das Recht, das Arbeitsergebnis automatisiert durch andere Software bzw. Roboter sowie in jeder beliebigen Hard- und Software- und Systemumgebung, auch zusammen mit anderer Software, zu nutzen
- das Nutzungs-/ Zugriffsrecht durch bzw. für IT-Dienstleister (z.B. Service Provider, Host Provider), die von dem Auftraggeber oder dem Endkunden beauftragt sind oder werden, um das Arbeitsergebnis für den Auftraggeber und/oder den Endkunden zu hosten, zu betreiben, zu verwalten oder sonstige outgesourcte Services zu erbringen (z.B. Rechenzentrums-Outsourcing, Nutzungsbereitstellung des Arbeitsergebnisses in Form des Application-Service-Providing-Modells (ASP), Cloud-Computing)

1.4

Soweit die Vertragsleistung in der Überlassung von schutzfähigen Werken und/oder sonstigen Entwicklungsergebnissen (z.B. zugrunde liegende Erkenntnisse, Konzepte, Methoden, Know-how, Beschreibungen) besteht bzw. diese umfasst, die vom Auftragnehmer oder von einem Dritten (z.B. Softwarehersteller) (i) bereits vor dem Inkrafttreten dieses Projektvertrags erstellt worden sind oder (ii) während der Laufzeit dieses Projektvertrages unabhängig von den Vertragsleistungen und ohne Verwendung des durch diesen Projektvertrag durch den Auftragnehmer erworbenen Know-Hows, der diesem Projektvertrag zugrunde liegenden Erkenntnisse, der in diesem Projektvertrag übermittelten oder erstellten Konzepte, Methoden und Beschreibungen etc. erstellt werden (nachfolgend „vorbestehende Werke“ genannt), insbesondere Standardsoftware, räumt der Auftragnehmer dem Auftraggeber sowie dem Endkunden an diesen vorbestehenden Werken ein einfaches, unwiderrufliches, übertragbares und inhaltlich, räumlich und zeitlich unbeschränktes Recht ein, die vorbestehenden Werke bestimmungsgemäß im Sinne des Vertragszwecks (vgl. insbesondere **Anlage 4, Leistungsbeschreibung**) zu nutzen. Das Nutzungsrecht des Auftraggebers bzw. Endkunden beinhaltet insbesondere auch das Recht, vorbestehende Werke auch für Zwecke des bzw. eines anderen Endkunden zu nutzen.

1.5

Nutzungs- und Verwertungsrechte, die dem Kunden auf Grundlage dieses Projektvertrages eingeräumt werden, sind Bestandteil der im Rahmen dieses Projektvertrages zu zahlenden Vergütung und werden von den Parteien als angemessen angesehen.

1.6

Die Rechtseinräumung i.S.d. Ziffer 1 umfasst ausdrücklich auch die Nutzungsrechte für bisher unbekannte Nutzungsarten mit der Maßgabe, dass das in diesen Fällen bestehende gesetzliche Widerrufsrecht des geistigen Eigentümers/ Urhebers unberührt bleibt.

1.7

Die in dieser Ziffer 1 dem Auftraggeber und dem Endkunden eingeräumten Nutzungs- und Verwertungsrechte gelten auch für

a) etwaige durch den Auftragnehmer zur Nutzung bereitgestellten neue Releases, Updates und Upgrades bereitgestellter Software sowie

b) die Programmdokumentation im Sinne der vorstehenden Ziffer 1.2 dieses Projektvertrags sowie die Dokumentation gemäß **Anlage 4, Leistungsbeschreibung**.

1.8

Sollte dieser Projektvertrag und/oder ein Einzelauftrag vorzeitig gekündigt werden, steht dem Kunden und dessen Endkunden das Recht zu, die bereits bis dahin entwickelten Arbeitsergebnisse bzw. vorbestehenden Werke im Sinne dieser Ziffer 1 weiterhin zu nutzen und zu verwerten.

1.9

Soweit die Vertragsleistungen Rechte Dritte enthalten, stellt der Auftragnehmer sicher, dass diese im gleichen Umfang wie in dieser Ziffer 1 vereinbart, an den Kunden übertragen bzw. diesem und dem Endkunden eingeräumt werden. Bei Einzelaufträgen finden urheberrechtliche Nutzungsrechteregelungen in den Bestimmungen des Auftragnehmers und/oder des Herstellers nur insoweit Anwendung, als dass diese den Bestimmungen und dem Vertragszweck dieses Projektvertrages und des jeweiligen Einzelauftrags nicht entgegenstehen und überdies für den Kunden bzw. Endkunden zumutbar sind bzw. diesen nicht unangemessen einschränken.

2 Open Source

2.1

Der Auftragnehmer stellt sicher, dass im Rahmen der Erbringung der Vertragsleistungen ausschließlich die in **Anhang 9** aufgeführte „Open Source Software“ eingesetzt wird. "Open Source Software“ im Sinne dieser Regelung ist Software, die von dem bzw. den Rechteinhaber(n) beliebigen Nutzern lizenzgebührenfrei mit dem Recht zur Bearbeitung und/oder Verbreitung auf der Grundlage einer Lizenz oder anderen vertraglichen Regelung überlassen wird (z.B. GNU General Public License (GPL), GNU Lesser GPL (LGPL), BSD License, Apache License, MIT License). Enthalten die Vertragsleistungen des Auftragnehmers Open Source Software, so hat der Auftragnehmer dem Auftraggeber zum Zeitpunkt der Bekanntgabe mindestens Folgendes zu liefern:

- Source Code der verwendeten Open Source Software, soweit die anwendbaren Open Source Lizenzbedingungen die Offenlegung dieses Source Codes verlangen
- Auflistung sämtlicher verwendeter Open Source Dateien mit einem Hinweis auf die jeweils anwendbare Lizenz sowie eine Kopie des vollständigen Lizenztextes

Etwaige darüberhinausgehende Pflichten des Auftragnehmers ergeben sich aus den jeweiligen Open Source Software-Lizenzbestimmungen.

2.2

Der Auftragnehmer versichert, dass durch die Verwendung der in der **Anhang 9** aufgeführten Open Source Software weder die Vertragsleistungen des Auftragnehmers, insbesondere in Form von Produkten und Arbeitsergebnissen, die im Rahmen der Vertragserbringung durch den Auftragnehmer entstehen, noch andere Produkte etc., die der Auftraggeber bzw. Endkunde im Zusammenhang mit der Nutzung der Vertragsleistungen des Auftragnehmers einsetzt bzw. nutzt,

einem sog. „Copyleft-Effekt“ unterliegen. Copyleft-Effekt bezeichnet hierbei jede vertragliche Regelung einer Open Source Lizenz, welche als Rechtsfolge anordnet, dass die jeweilige Open Source Lizenz der verwendeten Open Source Software-Komponente auch auf weiteren Code angewendet werden muss. Als „Copyleft-Effekt“ wird der Eintritt dieser Rechtsfolge bezeichnet.

2.3

Zudem versichert der Auftragnehmer, dass der Auftraggeber die Open Source Produkte als Teil der Vertragsleistungen im Sinne des Vertragszweckes nutzen, bearbeiten und einsetzen darf.

3 Informationspflichten des Auftragnehmers

3.1

Der Auftragnehmer verpflichtet sich, den Endkunden auf dessen Verlangen im Hinblick auf die Einhaltung der vertraglich vereinbarten Bedingungen zur Vertraulichkeit, Geheimschutz, Militärische Sicherheit, Korruptionsprävention und Datenschutz direkt zu informieren.

3.2

Der Auftragnehmer wird die von dem Auftraggeber zur Verfügung gestellten Informationen, Vorarbeiten, Unterlagen und Daten, soweit in diesem Projektvertrag oder dem jeweiligen Einzelauftrag nicht eine andere Frist festgelegt ist, unverzüglich prüfen. Erkennt der Auftragnehmer eine Unrichtigkeit, Unvollständigkeit oder Widersprüchlichkeit, so hat er den Auftraggeber unverzüglich darauf hinzuweisen.

3.3

Der Auftragnehmer wird dem Auftraggeber unverzüglich alle für die Leistungserbringung wesentlichen Informationen zur Verfügung stellen, insbesondere, wenn eine Vorgabe oder Forderung des Auftraggebers oder eine sich aus den vertraglichen Pflichten des Auftragnehmers ergebende Handlung in wesentlichem Umfang fehlerhaft, unvollständig, widersprüchlich oder nicht wie vereinbart ausführbar ist.

3.4

Der Auftragnehmer verpflichtet sich insbesondere, den Auftraggeber unverzüglich zu unterrichten, sobald ein Gläubiger des Auftragnehmers die Zwangsvollstreckung in die Geschäftsanteile des Auftragnehmers oder von mit ihm verbundenen Unternehmen betreibt. Beabsichtigt der Auftragnehmer die Stellung eines Vergleichs- oder Insolvenzantrages, so hat er dies dem Auftraggeber unverzüglich in Textform mitzuteilen. Das gleiche gilt, wenn der Auftragnehmer beabsichtigt, sein Unternehmen aufzugeben oder wenn eine nicht vorübergehende Zahlungseinstellung absehbar wird.

4 Vertraulichkeit, Geheimhaltung

4.1

Der Auftragnehmer hat alle im Zusammenhang mit der Erbringung der Vertragsleistungen erlangten Informationen des Auftraggebers, des Kunden bzw. des Endkunden über rechtliche, betriebliche, geschäftliche, technische oder wissenschaftliche Angelegenheiten und sonstige Informationen im Sinne der Richtlinie (EU) 2016/943 bzw. des Gesetzes zur Umsetzung der

Richtlinie (EU) 2016/943 (Geschäftsgeheimnisgesetz), die nicht offenkundig sind, vertraulich zu behandeln. Dies gilt unabhängig davon, ob die Informationen als vertraulich gekennzeichnet sind oder nicht. Unerheblich ist zudem, auf welche Weise und in welcher Form sie zur Kenntnis gelangt sind.

4.2

Die in dieser Ziffer vorstehend begründete Geheimhaltungs- bzw. Vertraulichkeitspflicht gilt nicht für vertrauliche Informationen,

c) die bereits zum Zeitpunkt der Offenlegung öffentlich bekannt waren

d) die nach Offenlegung durch Veröffentlichung oder auf andere Weise, ausgenommen durch Verletzung der Bestimmungen dieses Projektvertrages, öffentlich bekannt werden

e) die dem Auftragnehmer von einem Dritten bekannt gegeben worden sind, ohne dass dies auf einer Verletzung der Bestimmungen dieses Projektvertrages beruht

f) zu deren Bekanntgabe an Dritte der Auftragnehmer gesetzlich, aufgrund einer gerichtlichen oder behördlichen Anordnung verpflichtet ist, wobei der Auftragnehmer den Auftraggeber hiervon in Kenntnis zu setzen, ihm eine Einschätzung über die Zurückweisungsmöglichkeiten zur Verfügung zu stellen bzw. alle erforderlichen Maßnahmen zum Schutz und zur Begrenzung der Offenlegung vorzunehmen hat

4.3

Der Auftragnehmer ist zur Verschwiegenheit über alle vertraulichen Informationen des Kunden und des Endkunden – auch über die Laufzeit dieses Projektvertrages bzw. des Einzelauftrags hinaus – verpflichtet. Er darf sie ausschließlich zum Zweck der Auftragsausführung einsetzen und auch nur zu diesem Zweck Aufzeichnungen darüber erstellen. Schriftstücke und Datenträger mit vertraulichen Informationen sind gegen unberechtigte Kenntnisnahme zu sichern. Die Informationen dürfen nur an Personen weitergegeben werden, die ihrerseits zur Verschwiegenheit verpflichtet worden sind und die zum Zweck der Auftragsausführung von den Informationen Kenntnis erhalten müssen.

Der Auftragnehmer erklärt sich dazu bereit, dafür Sorge zu tragen, dass die zur Erbringung der Vertragsleistungen eingesetzten Personen sich auf ausdrückliches Verlangen des Auftraggebers persönlich gegenüber dem Kunden durch eine entsprechende Vereinbarung zur Verschwiegenheit verpflichten.

Bei Verlust vertraulicher Informationen ist unverzüglich der Auftraggeber zu benachrichtigen.

4.4

Nach entsprechender Aufforderung hat der Auftragnehmer alle Schriftstücke und Datenträger mit vertraulichen Informationen an den Auftraggeber bzw. Kunden / Endkunden nach Wahl des Auftraggebers herauszugeben bzw. zu vernichten, soweit dem keine gesetzlichen Aufbewahrungsvorschriften entgegenstehen.

4.5

Sämtliche vom Auftragnehmer eingesetzten Personen sind vor der Leistungserbringung in Textform auf die Vertraulichkeit zu verpflichten.

4.6

Der Auftragnehmer ist zudem zur Verschwiegenheit über fremde, zum persönlichen Lebensbereich gehörende Geheimnisse im Sinne von § 203 StGB verpflichtet, die ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit bekannt werden (z.B. in IT-Systemen der Bundeswehrkrankenhäuser gespeicherte Patientendaten). Seine Unterauftragnehmer hat der Auftragnehmer entsprechend zu verpflichten, wenn die Möglichkeit der Kenntnisnahme von Geheimnissen besteht. Gleiches gilt für das vom Auftragnehmer zur Leistungserbringung eingesetzte Personal, wenn die Möglichkeit der Kenntnisnahme von Geheimnissen besteht. Ein Verstoß gegen das Verpflichtungserfordernis ist ebenso wie das Offenbaren von Privatgeheimnissen strafbar gemäß § 203 Abs. 4 StGB.

4.7

Anderweitige Verpflichtungen des Auftragnehmers zu Vertraulichkeit und Geheimhaltung, insbesondere solche aufgrund weiterer vertraglicher und gesetzlicher Geheimhaltungsvorschriften bleiben unberührt.

4.8

Für Presseerklärungen und für jede andere öffentlich zugängliche Verlautbarung (z. B. Werbung oder die Angabe als Referenzprojekt) durch den Auftragnehmer, die im Zusammenhang mit dieser Vereinbarung stehen, ist beim Auftraggeber eine vorherige Erlaubnis in Textform einzuholen. Der Auftraggeber kann diese Erlaubnis jederzeit ohne Angabe von Gründen widerrufen.

5 Zulässige Informationsweitergabe

5.1

Der Auftragnehmer stimmt einer Weitergabe von Informationen im Zusammenhang mit diesem Projektvertrag und den darunter geschlossenen Einzelaufträgen an den Deutschen Bundestag im Rahmen seines Informations- und Auskunftsrechts gegenüber der Bundesregierung sowie an sonstige Verfassungsorgane im Rahmen der Ausübung ihrer Prüfungs- und Kontrollrechte zu.

5.2

Soweit in diesem Zusammenhang Betriebs- und Geschäftsgeheimnisse des Auftragnehmers betroffen sind, weist der Auftraggeber bei der Übermittlung von Informationen i.S.d. Ziffer 5.1 ausdrücklich darauf hin, dass die empfangende Stelle durch geeignete Maßnahmen sicherzustellen hat, dass die Regelungen des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) zum Schutz der Geschäftsgeheimnisse der Auftragnehmer beachtet werden.

5.3

Der Auftragnehmer wird in gleicher Weise die Zustimmung seiner Unterauftragnehmer einholen.

6 Informationssicherheit

6.1

Der Auftragnehmer verpflichtet sich, bei der Vertragserfüllung alle Maßnahmen zu treffen, die zur Sicherstellung der IT-Sicherheit nach den gesetzlichen Bestimmungen erforderlich sind, sowie

den IT-Sicherheitsanweisungen des Auftraggebers bzw. des Kunden/Endkunden Folge zu leisten. Darüber hinaus sind die „Anforderungen an die Informationssicherheit der BWI“ **(Anhang 1)** während der Laufzeit des Projektvertrages und der hierunter abgeschlossenen Einzelaufträge einzuhalten.

6.2

Soweit im Projektvertrag, seinen Anlagen und Anhängen oder im Einzelauftrag weitere Anforderungen und/oder Regeln der Informationssicherheit enthalten sind, wird der Auftragnehmer diese Anforderungen und Regeln nach Maßgabe der dort vorgegebenen Festlegungen während der Laufzeit des Projektvertrages und der hierunter abgeschlossenen Einzelaufträge einhalten.

7 Datenschutz

7.1

Der Auftragnehmer sorgt dafür, dass alle Personen, die von ihm im Rahmen der Vertragserfüllung betraut sind, die gesetzlichen Bestimmungen über den Datenschutz beachten, insbesondere die Datenschutzvorschriften der Europäischen Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG).

7.2

Soweit der Auftragnehmer personenbezogene Daten des Kunden im Auftrag des Auftraggebers im Rahmen des Projektvertrages oder eines Einzelauftrages i.S.d. Art. 28 DSGVO verarbeitet, schließen die Parteien eine Auftragsverarbeitungsvereinbarung gemäß der **Anhang 2** der Projektvereinbarung.

7.3

Für den Fall, dass ein Einzelauftrag die Verarbeitung personenbezogener Daten des Endkunden vorsieht oder erfordert oder eine Tätigkeit, bei der der Auftragnehmer in anderer Weise Zugang zu personenbezogenen Daten des Endkunden erhalten kann, steht die Wirksamkeit des Einzelauftrags unter dem Vorbehalt der Zustimmung des Endkunden des Auftraggebers hinsichtlich der Einbindung des Auftragnehmers. Im Falle der Zustimmung des Endkunden zur Verarbeitung seiner personenbezogenen Daten im Auftrag i.S.d. Art. 28 Abs. 4 DSGVO, schließen die Parteien eine Auftragsverarbeitung gemäß **Anhang 3** der Projektvereinbarung.

8 Verschlussachen / Sabotageschutz / Militärische Sicherheit

8.1

Verschlusssachen (nachfolgend „VS“ genannt) sind alle im öffentlichen Interesse geheimhaltungsbedürftigen Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform, die durch besondere Sicherungsmaßnahmen vor Unbefugten geheim gehalten werden müssen. Sie werden entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle des Bundes oder auf deren Veranlassung in Geheimhaltungsgrade eingestuft. Der Auftragnehmer ist verpflichtet, über den gesamten Leistungszeitraum sowie nach Kündigung, Auflösung oder Ablauf des Projektvertrages bzw. Einzelauftrages den Schutz aller in seinem Besitz befindlichen oder ihm zur Kenntnis gelangten Verschlusssachen gemäß den einschlägigen Rechts- und Verwaltungsvorschriften zu gewährleisten. Seine Unterauftragnehmer hat er entsprechend zu verpflichten.

8.2

Für den Fall, dass er bei der Leistungserbringung Zugang zu Verschlusssachen des Geheimhaltungsgrades „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (nachfolgend „VS-NfD“ genannt) erhält oder er VS-NfD be- oder verarbeitet, verpflichtet sich der Auftragnehmer, das VS-NfD-Merkblatt nebst Anlage in der zum Zeitpunkt des Vertragsabschlusses gültigen Fassung strikt zu befolgen und einen Ansprechpartner zu benennen (**Anhang 4**). Der Auftragnehmer wird dafür sorgen, dass alle eigenen Mitarbeiter und Mitarbeiter von Unterauftragnehmern, die VS-NfD zur Kenntnis erhalten könnten, dieses VS-NfD-Merkblatt erhalten und beachten werden sowie den Erhalt dokumentieren.

8.3

Der Auftragnehmer verpflichtet sich darüber hinaus, zusätzliche Sperrvermerke zu VS (z.B. „Nur Deutschen zur Kenntnis“) zu beachten und in der Leistungskette umzusetzen und einzuhalten.

Für den Fall, dass der Auftraggeber oder der Kunde/Endkunde den Einsatz von sicherheitsüberprüftem Personal fordert, weil davon auszugehen ist, dass die Leistungserbringung an sicherheitsempfindlichen Stellen zu erfolgen hat (Sabotageschutz) und/oder Zugang zu Verschlusssachen des Geheimhaltungsgrades „VS-Vertraulich“ oder höher besteht (Geheimschutz), hat der Auftragnehmer sicherzustellen, dass für diese Leistungsanteile nur entsprechend sicherheitsüberprüftes Personal eingesetzt wird.

8.4

Soweit vom Auftraggeber oder seinem Kunden/Endkunden gefordert, hat der Auftragnehmer an der Geheimschutzbetreuung durch das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) teilzunehmen. Der Auftragnehmer ist verpflichtet, rechtzeitig alle Mitwirkungshandlungen vorzunehmen, die für eine Aufnahme in die Geheimschutzbetreuung bzw. die Aufrechterhaltung der Geheimschutzbetreuung notwendig sind. Die Bestimmungen des Geheimschutzhandbuches („Handbuch für den Geheimschutz in der Wirtschaft“ – nachfolgend „GHB“ genannt) sind vom Auftragnehmer zu beachten und alle erforderlichen organisatorischen, personellen und materiellen Geheimschutzmaßnahmen nach Maßgabe des GHB zu treffen. Insbesondere hat der Auftragnehmer die aus Geheimschutzgründen erforderlichen Sicherheitsüberprüfungen zu veranlassen.

8.5

Das Personal des Auftragnehmers darf militärische Bereiche (Anlagen, Einrichtungen und Schiffe) des Endkunden Bundeswehr und der verbündeten Streitkräfte in der Bundesrepublik Deutschland nur nach rechtzeitiger vorheriger Ankündigung beim Verantwortlichen, im Allgemeinen dem Sicherheitsbeauftragten der zu besuchenden Stelle, betreten. Nach entsprechender Aufforderung hinterlegt der Auftragnehmer eine Namensliste des eingesetzten Personals (mit Angaben zu Name, Vorname, Geb.-Datum, Geb.-Ort, Staatsangehörigkeit, Reisepass- oder Personalausweis-Nr., Ausstellungsdatum, Ausstellungsort, Wohnanschrift, Arbeitgeber) bei dem verantwortlichen Sicherheitsbeauftragten der jeweiligen Liegenschaft und gibt die verantwortlichen Aufsichtspersonen des Auftragnehmers namentlich bekannt.

8.6

Der Auftragnehmer verpflichtet sich, das von ihm eingesetzte Personal vor einer Leistungserbringung innerhalb eines militärischen Bereiches im erforderlichen Umfang über die allgemeinen und speziellen Vorschriften zur Wahrung der militärischen Sicherheit zu informieren.

8.7

Der Auftragnehmer ist verpflichtet, Forderungen des BMWK, des Auftraggebers und/oder seines Kunden/Endkunden hinsichtlich der Sicherheit und der Geheimhaltung bei der Leistungserbringung nachzukommen und auf deren Verlangen bei Vorliegen zwingender Gründe bestimmte Personen von der Vertragsdurchführung fernzuhalten.

8.8

Abweichungen von den Bestimmungen des Geheimschutzhandbuches oder des VS-NfD-Merkblattes bedürfen ebenso wie die Weitergabe von Verschlusssachen der Zustimmung des Auftraggebers bzw. seines Kunden/Endkunden.

8.9

Nach Beendigung der VS-Arbeiten oder nach entsprechender Aufforderung hat der Auftragnehmer die im Zusammenhang mit diesem Vertrag erhaltenen VS-Dokumente und VS-Datenträger dem Auftraggeber bzw. seinem Kunden/Endkunden zu übergeben oder mit dessen Zustimmung zu vernichten.

9 Verhaltenskodex

9.1

Der Auftragnehmer ist verpflichtet, die im Rahmen der Erbringung der Vertragsleistungen anwendbaren Gesetze einzuhalten. Insbesondere wird er sich weder aktiv noch passiv, direkt oder indirekt an jeder Form der Bestechung, der Verletzung der Grundrechte seiner Arbeitnehmerinnen und Arbeitnehmer (nachfolgend einzeln oder gemeinsam „Arbeitnehmer“ genannt) oder der Menschenrechte beteiligen. Der Auftragnehmer verpflichtet sich zudem, auch die Vorschriften des Mindestlohngesetzes („Gesetz zur Regelung eines allgemeinen Mindestlohns“ – MiLoG) und die Regelungen des Arbeitnehmer-Entsendegesetzes ("Gesetz über zwingende Arbeitsbedingungen für grenzüberschreitend entsandte und für regelmäßig im Inland beschäftigte Arbeitnehmer und Arbeitnehmerinnen" – AEntG) einzuhalten, sofern für ihn einschlägig. Der Auftragnehmer stellt den Auftraggeber und seinen Kunden / Endkunden von sämtlichen Ansprüchen frei, die im Falle eines Verstoßes des Auftragnehmers oder eines seiner Unterauftragnehmer gegen die Vorschriften des MiLoG gegen den Auftraggeber aus der Bürgenhaftung gemäß § 13 MiLoG i.V.m. § 14 AEntG geltend gemacht werden.

9.2

Der Auftragnehmer wird im Übrigen Verantwortung für die Gesundheit und Sicherheit seiner Arbeitnehmer am Arbeitsplatz übernehmen, insbesondere wird er, sofern Leistungen an Standorten des Auftraggebers oder Liegenschaften eines Endkunden des Auftraggebers erbracht werden, die ihm bekanntgemachten Arbeitsschutzvorschriften (z.B. Arbeitsschutzmerkblätter) einhalten.

9.3

Der Auftraggeber erwartet von dem Auftragnehmer die Einhaltung seiner folgenden menschenrechtlichen und umweltbezogenen Vorgaben bei der Erbringung sämtlicher Vertragsleistungen für den Auftraggeber (nachfolgend „menschenrechtliche und umweltbezogene Erwartungen“ genannt).

9.3.1

Es darf keine Zwangsarbeit, Sklavenarbeit oder derart vergleichbare Arbeit eingesetzt werden. Jede Arbeit für den Auftragnehmer muss freiwillig und ohne Androhung von Strafe erfolgen. Arbeitnehmer müssen jederzeit das Beschäftigungsverhältnis beenden können. Außerdem darf keine inakzeptable Behandlung von Arbeitskräften, wie etwa psychische Härte, sexuelle und persönliche Belästigung und Erniedrigung stattfinden.

9.3.2

Es darf keine Kinderarbeit eingesetzt werden. Der Auftragnehmer ist aufgefordert, sich an die Empfehlung aus den ILO-Konventionen zum Mindestalter für die Beschäftigung von Kindern zu halten. Demnach darf das Alter der Arbeitnehmer nicht geringer sein als das Alter, mit dem nach dem Recht des Beschäftigungsortes die allgemeine Schulpflicht endet und in jedem Fall nicht unter 15 Jahre. Die Rechte junger Arbeitnehmer sind zu schützen: Unter 18 Jahren dürfen sie nicht für Arbeiten eingesetzt werden, die schädlich für die Gesundheit, Sicherheit oder Sittlichkeit von Kindern sind. Besondere Schutzvorschriften sind einzuhalten.

9.3.3

Die geltenden Gesetze, Vorschriften und Normen zum Arbeitsschutz, zur Arbeitssicherheit und zum Gesundheitsschutz werden eingehalten. Der Auftragnehmer ist verpflichtet, seinen Arbeitnehmern eine sichere und gesunde Arbeitsumgebung zu ermöglichen. Übermäßige körperliche oder geistige Ermüdung sind durch geeignete Maßnahmen zu verhindern. Zudem werden die Arbeitnehmer regelmäßig über geltende Gesundheitsschutz- und Sicherheitsnormen sowie -maßnahmen informiert und geschult. Den Arbeitnehmern wird der Zugang zu Trinkwasser in ausreichender Menge ermöglicht sowie der Zugang zu sauberen sanitären Einrichtungen.

9.3.4

Das Entgelt für reguläre Arbeitsstunden und Überstunden muss dem nationalen gesetzlichen Mindestlohn oder den branchenüblichen Mindeststandards entsprechen, je nachdem, welcher Betrag höher ist. Den Arbeitnehmern sind alle gesetzlich vorgeschriebenen Leistungen zu gewähren. Das Vorenthalten eines angemessenen Lohns oder Lohnabzüge als Strafmaßnahmen sind nicht zulässig. Der Auftragnehmer hat sicherzustellen, dass die Arbeitnehmer klare, detaillierte und regelmäßige Informationen über die Zusammensetzung ihres Entgelts in Textform erhalten.

9.3.5

Das Recht der Arbeitnehmer, Organisationen ihrer Wahl zu gründen, ihnen beizutreten, und Kollektivverhandlungen zu führen und zu streiken, ist zu respektieren. In Fällen, in denen die Vereinigungsfreiheit und das Recht zu Kollektivverhandlungen gesetzlich eingeschränkt sind, sind alternative Möglichkeiten eines unabhängigen und freien Zusammenschlusses der Arbeitnehmer zum Zweck von Kollektivverhandlungen einzuräumen. Arbeitnehmervertreter sind vor Diskriminierung zu schützen. Arbeitnehmer dürfen nicht aufgrund von Gründung, Beitritt oder Mitgliedschaft in einer solchen Organisation diskriminiert werden. Arbeitnehmervertretern ist freier Zugang zu den Arbeitsplätzen ihrer Kollegen zu gewähren, um sicherzustellen, dass sie ihre Rechte in gesetzmäßiger und friedlicher Weise wahrnehmen können.

9.3.6

Die Diskriminierung und Ungleichbehandlung von Arbeitnehmern in jeglicher Form ist unzulässig, soweit sie nicht in den Erfordernissen der Arbeitnehmer begründet ist. Dies gilt z. B. für

Benachteiligungen aufgrund von Geschlecht, Rasse, nationaler, ethnischer oder sozialer Herkunft, Hautfarbe, Behinderung, Gesundheitsstatus, politischer Überzeugung, Herkunft, Weltanschauung, Religion, Alter, Schwangerschaft oder sexueller Orientierung. Die persönliche Würde, Privatsphäre und Persönlichkeitsrechte jedes Einzelnen werden respektiert.

9.3.7

Der Auftragnehmer führt keine schädliche Bodenveränderung, Gewässerverunreinigung, Luftverunreinigung, schädliche Lärmemission oder übermäßigen Wasserverbrauch herbei, welche die natürlichen Grundlagen zum Erhalt und der Produktion von Nahrung erheblich beeinträchtigt, einer Person den Zugang zu einwandfreiem Trinkwasser verwehrt, einer Person den Zugang zu Sanitäranlagen erschwert oder zerstört oder die Gesundheit einer Person schädigt.

9.3.8

Die widerrechtliche Zwangsräumung und der widerrechtliche Entzug von Land, Wäldern und Gewässern bei dem Erwerb, der Bebauung oder anderweitiger Nutzung von Land, Wäldern und Gewässern, deren Nutzung die Lebensgrundlage einer Person sichert, ist verboten.

9.3.9

Die Beauftragung privater oder öffentlicher Sicherheitskräfte ist untersagt, wenn aufgrund mangelnder Unterweisung oder Kontrolle bei dem Einsatz des Sicherheitsunternehmens das Verbot von Folter missachtet wird, Leib oder Leben verletzt werden oder die Vereinigungs- und Koalitionsfreiheit beeinträchtigt wird.

9.3.10

Der Auftragnehmer wird auch über die vorgenannten Verbote hinaus nichts tun oder pflichtwidrig unterlassen, das unmittelbar geeignet ist, in besonders schwerwiegender Weise eine der geschützten Rechtsposition zu beeinträchtigen, und dessen Rechtswidrigkeit bei verständiger Würdigung aller in Betracht kommenden Umstände offensichtlich ist.

9.3.11

Der Auftragnehmer hält die jeweils anwendbaren Umweltschutzgesetze und Umweltverordnungen ein. Der Auftragnehmer gewährleistet, dass alle erforderlichen Umweltgenehmigungen vorliegen und auf aktuellem Stand gehalten und in seinem Unternehmen befolgt werden.

9.3.12

Der Auftragnehmer wird sich bemühen, seine CO2-Bilanz zu senken, um dadurch zur Erreichung der Klimaziele der Klimakonferenz von Paris beizutragen.

9.3.13

Der Auftragnehmer wird gefährliche Stoffe und Chemikalien kennzeichnen und die sichere Handhabung, Lagerung, den sicheren Transport und die sichere Entsorgung gewährleisten. Der Auftragnehmer ist verpflichtet, alle Produktsicherheitsanordnungen einzuhalten.

9.3.14

Der Auftragnehmer stellt keine mit Quecksilber versetzten Produkte her, verwendet kein Quecksilber sowie keine Quecksilberverbindungen und behandelt Quecksilberabfälle gemäß dem Minamata-Übereinkommen. Ferner produziert und verwendet der Auftragnehmer keine

Chemikalien, handhabt die Sammlung, Lagerung und Entsorgung von Abfällen umweltgerecht nach dem POPs-Übereinkommen. Zudem befolgt der Auftragnehmer insbesondere das Verbot der Ausfuhr, Verbringung und Entsorgung gefährlicher Abfälle nach dem Baseler Übereinkommen.

9.3.15

Der Auftragnehmer verpflichtet sich, im Rahmen einer Nachhaltigkeitsstrategie das ökologische Gleichgewicht zu erhalten, schädliche Umweltbelastungen nach Möglichkeit zu vermeiden oder jedenfalls zu vermindern und natürliche Ressourcen zu schonen. Es wird erwartet, dass der Auftragnehmer sämtliche geltenden lokalen und internationalen anerkannten Umweltstandards und Gesetze selbst anerkennt und einhält.

9.3.16

Der Auftragnehmer nimmt seine ökologische Verantwortung über die gesamte Lieferkette wahr und setzt diese sowohl hinsichtlich seiner Produkte und Dienstleistungen als auch hinsichtlich der von ihm verwendeten Verpackungen um.

9.4

Liefert der Auftragnehmer Vertragsprodukte, die Anteile enthalten, die aufgrund von internationalen und/oder nationalen Gesetzen, EU-Verordnungen und/oder EU-Richtlinien stofflichen Restriktionen und/oder stofflichen Informationspflichten unterliegen, hat der Auftragnehmer diese Stoffe durch ein von den Parteien vereinbartes, angemessenes Format spätestens zum Zeitpunkt der ersten Lieferung entsprechend zu deklarieren. Das Vorstehende gilt nur für die jeweils aktuellen Gesetze, EU-Richtlinien und/oder EU-Verordnungen, die am Geschäftssitz des Auftragnehmers oder des Auftraggebers oder am vereinbarten Liefer- und Leistungsort Anwendung finden.

9.5

Im Fall der Leistungserbringung für den Endkunden Bundeswehr finden die folgenden Dokumente Anwendung: „Empfehlung zur Korruptionsprävention“ (**Anhang 5a)**, „Richtlinie zur Korruptionsprävention“ (**Anhang 5b),** „Umsetzung der Richtlinie zur Korruptionsprävention“ (**Anhang 5c)**, sowie die „Zentrale Dienstvorschrift zur Annahme von Zuwendungen“ (**Anhang 6)**. Darüber hinaus gilt die Antikorruptionsklausel „Interimsfassung der Nrn. 11.4 und Nr. 11.5 der zusätzlichen Vertragsbedingungen des Bundesministeriums der Verteidigung zur Verdingungsordnung für Leistungen Teil B, ZVB/BMVg) vom 28.01.2005“ (**Anhang 7)**. Auf die dort enthaltene Vertragsstrafenregelung wird ausdrücklich hingewiesen.

9.6

Sofern aufgrund der dem Auftragnehmer übertragenen Aufgaben die Möglichkeit des Geheimnisbruchs oder der Verwirklichung der in **Anhang 8** sonst genannten Vorschriften denkbar ist, erklärt der Auftragnehmer zudem seine Bereitschaft, sich auf Verlangen des Auftraggebers oder seines Endkunden auf die gewissenhafte Erfüllung seiner Obliegenheiten nach Maßgabe des Verpflichtungsgesetzes in seiner jeweils gültigen Fassung gemäß **Anhang 8** verpflichten zu lassen. Der Auftragnehmer hat dafür Sorge zu tragen, dass auch das zur Leistungserbringung eingesetzte Personal sich mit der Verpflichtung einverstanden erklärt, was zur Anwendung der für Amtsträger geltenden Strafvorschriften des Strafgesetzesbuches führt. Dies gilt insbesondere für zur Leistungserbringung eingesetzte Personen, denen im Rahmen des Zugangs zu einem IT-System (z.B. bei der Softwarepflege) strafrechtlich geschützte Geheimnisse bekannt werden bzw.

die auf die Ausführung von Aufgaben der öffentlichen Verwaltung durch die Art der vertraglichen Leistung (z.B. Unterstützungs- oder Beratungsleistungen) objektiv Einfluss nehmen können. Der nach dieser Ziffer 9.6 zu verpflichtende Personenkreis kann im Einzelfall durch den Auftraggeber zu benennende Personen umfassen, die folgende oder vergleichbare Funktionen wahrnehmen:

- Angehörige der Geschäftsführung
- Abteilungsleitungen
- Projektleitungen
- Mitarbeiterinnen/Mitarbeiter, die sich nicht nur vorübergehend in der Dienststelle eines Endkunden aufhalten (z.B. im Rahmen von Unterstützungsleistungen bei IT-Projekten)
- Geschäfts-/ Betriebsinhaber (etwa Einzelunternehmer, freiberuflich Tätige), deren Mitwirkung bei der Abwicklung des Auftragsverhältnisses nicht ausgeschlossen werden kann
- Personal, das mit Vorbereitung und Durchführung von Vergabeverfahren für den Auftraggeber befasst ist
- alle sonstigen Personen, die bei einer Gesamtbetrachtung die Möglichkeit des Einblicks oder einer Einflussnahme auf die Ausführung von Aufgaben der öffentlichen Verwaltung haben

Der Auftragnehmer verpflichtet sich, auf Verlangen des Auftraggebers den betroffenen Personenkreis namentlich unter Angabe des Aufgabenbereiches/ der Funktion zu benennen und Personalveränderungen (Neueinstellungen, Ausscheiden aus dem Beschäftigungsverhältnis etc.) zur Weitergabe an die zuständige Stelle des Endkunden mitzuteilen.

10 Lieferkettenmanagement

10.1

Dem Auftragnehmer ist bekannt, dass der Auftraggeber nach dem Lieferkettensorgfaltspflichtengesetz (LkSG), das am 1. Januar 2023 in Kraft tritt, zur Umsetzung von unternehmerischen Sorgfaltspflichten in seinen weltweiten Lieferketten verpflichtet ist. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen Verlangen unverzüglich kostenfrei alle beim Auftragnehmer vorhandenen Informationen zur Verfügung zu stellen, die der Auftraggeber zur Erfüllung seiner gesetzlichen Berichtspflicht im Rahmen der Berichterstellung gemäß dem LkSG benötigt.

10.2

Der Auftragnehmer sichert dem Auftraggeber ausdrücklich zu, seiner Verantwortung zur Wahrung der Menschenrechte und zum Schutz der Umwelt in den Lieferketten des Auftraggebers nachzukommen. Dazu verpflichtet sich der Auftragnehmer gegenüber dem Auftraggeber, dass er bei der Erfüllung seiner vertraglichen Pflichten gegenüber dem Auftraggeber stets die im Verhaltenskodex (Ziffer 9 des Projektvertrages) aufgeführten menschenrechtsbezogenen und umweltbezogenen Erwartungen des Auftraggebers einhält und den Auftraggeber unverzüglich informiert, sofern er ein menschenrechtliches oder umweltbezogenes Risiko im Sinne des § 2 LkSG im Zusammenhang mit einer Vertragsleistung bei sich und/oder einem seiner Unterauftragnehmer festgestellt hat.

10.3

Die nachfolgenden Ziffern 10.4 bis 10.6 des Projektvertrages finden im Verhältnis der Parteien nur Anwendung, wenn der Auftraggeber im Rahmen seiner Risikoanalyse ein menschenrechtliches oder umweltbezogenes Risiko im Sinne des § 2 LkSG im Zusammenhang mit einer Vertragsleistung des Auftragnehmers festgestellt hat.

10.4

Der Auftragnehmer verpflichtet seine unmittelbaren Zulieferer, welche in Verbindung mit ihren vertraglichen Leistungen für den Auftragnehmer mittelbar Vertragsleistungen für den Auftraggeber erbringen, zur Einhaltung der menschenrechtlichen und umweltbezogenen Erwartungen des Auftraggebers gemäß Ziffer 9 des Projektvertrages. Darüber hinaus wird der Auftragnehmer durch entsprechende vertragliche Vereinbarungen mit seinen unmittelbaren Zulieferern sicherstellen, dass diese in gleichem Umfang wie der Auftragnehmer im Verhältnis zum Auftraggeber die Einhaltung der menschenrechtlichen und umweltbezogenen Erwartungen des Auftraggebers an deren Zulieferer adressieren und diese Pflicht entlang der Lieferkette weitergeben.

10.5

Die Einhaltung der menschenrechtlichen und umweltbezogenen Erwartungen des Auftraggebers bei dem Auftragnehmer kann risikobasiert im Rahmen von Audits nach Maßgabe der Ziffer 12 vom Auftraggeber überprüft werden.

10.6

Der Auftragnehmer führt bei seinen Arbeitnehmern und bei seinen unmittelbaren Lieferanten Schulungen und Weiterbildungen zur Durchsetzung der vorgenannten vertraglichen Zusicherungen durch. Kommt der Auftragnehmer dieser Verpflichtung nicht oder nicht in angemessener Weise nach, ist der Auftraggeber berechtigt, diese Schulungen und Weiterbildungen bei dem Auftragnehmer auf dessen Kosten selbst durchzuführen oder durch einen externen Dienstleister durchführen zu lassen. Der Auftragnehmer wird dem Auftraggeber oder dem beauftragten Dritten in diesen Fällen in angemessenem Umfang die Durchführung der Schulungen ermöglichen. Er verpflichtet sich, bei der Umsetzung angemessen mitzuwirken.

10.7

Verletzt der Auftragnehmer die menschenrechtlichen und umweltbezogenen Erwartungen im Sinne der Ziffer 9 des Projektvertrages, wird dem Auftragnehmer vom Auftraggeber in Textform eine angemessene Frist gesetzt, um die Verletzung zu beenden oder – falls dies dem Auftragnehmer nicht möglich ist – durch angemessene Maßnahmen zu minimieren und das Verhalten in Einklang mit den Regelungen der Ziffer 9 des Projektvertrages zu bringen (nachfolgend „Abhilfe“ genannt). Ist eine Abhilfe in absehbarer Zeit nicht möglich, so hat der Auftragnehmer dies dem Auftraggeber anzuzeigen und gemeinsam mit dem Auftraggeber ein Konzept inklusive Zeitplan zur Beendigung oder Minimierung der Verletzung zu erstellen. Der Auftragnehmer ist verpflichtet, rechtzeitig alle Mitwirkungshandlungen vorzunehmen, die für die wirksame Abhilfe und die Umsetzung des Konzepts notwendig sind.

10.8

Hält der Auftragnehmer die menschenrechtlichen und umweltbezogenen Erwartungen des Auftraggebers nicht ein und verletzt eine in Ziffer 9 des Projektvertrages aufgeführte geschützte Rechtsposition oder umweltbezogene Pflicht, ist der Auftraggeber berechtigt, die Geschäftsbeziehung mit dem Auftragnehmer während der Bemühungen zur Risikominimierung

bzw. -beendigung gemäß Ziffer 10.7 unter Einstellung der Vergütung an den Auftragnehmer solange auszusetzen.

Der Auftraggeber ist ferner berechtigt, diesen Projektvertrag und die jeweils hiervon betroffenen Einzelaufträge ganz oder teilweise aus wichtigem Grund außerordentlich fristlos zu kündigen, wenn (i) die Verletzung einer geschützten Rechtsposition oder einer umweltbezogenen Pflicht vom Auftraggeber als schwerwiegend bewertet wird, (ii) die Umsetzung der gemäß Ziffer 10.7 erforderlichen Abhilfemaßnahmen nach Ablauf der hierfür festgelegten Frist nicht oder nicht vollständig erfolgt ist und (iii) keine milderen Mittel zur Verfügung stehen. Eine besonders schwerwiegende Verletzung ist insbesondere dann anzunehmen, wenn dem Betroffenen oder der Umwelt aufgrund der Verletzung ein erheblicher Schaden droht.

Andere oder weitergehende gesetzliche und/oder vertragliche Rechte bleiben unberührt.

10.9

Liegen dem Auftraggeber tatsächliche Anhaltspunkte vor, die eine Verletzung menschenrechtlicher und/oder umweltbezogener Erwartungen des Auftraggebers bei einem mittelbaren Zulieferer des Auftraggebers möglich erscheinen lassen, so verpflichtet sich der Auftragnehmer, den Auftraggeber dabei zu unterstützen, gegenüber diesem mittelbaren Zulieferer angemessene Präventionsmaßnahmen zu verankern.

11 Exportkontrollvorschriften, Genehmigungen

11.1

Die Ausfuhr von Lieferungen und Leistungen kann gemäß Ausfuhrbestimmungen der Bundesrepublik Deutschland und/oder der Europäischen Union (EU) und/oder anderer Staaten, insbesondere der USA, einer Genehmigungspflicht unterliegen.

11.2

Der Auftragnehmer ist verpflichtet, dem Auftraggeber innerhalb von vierzehn (14) Kalendertagen nach erster Anforderung die für die Einhaltung der jeweiligen Exportkontrollvorschriften notwendigen Angaben für jedes Produkt in Textform mitzuteilen. Die Angaben beinhalten die ECCN (Export Control Classification Number), AL-Nummer (Ausfuhrlisten-Nummer), die statistische Warennummer sowie die Maße, das Nettogewicht, das Bruttogewicht und den statistischen Warenwert. Auf Anfrage des Auftraggebers hat der Auftragnehmer zusätzlich und zeitnah zu jedem Produkt ein Ursprungszeugnis und/oder einen sonstigen Präferenznachweis zu übermitteln. Wird der Umfang des Vertragsgegenstandes dieses Projektvertrages nach Inkrafttreten erweitert, so hat der Auftragnehmer hierfür die entsprechenden Exportdaten (vom Lieferanten) in gleicher Weise mitzuteilen.

11.3

Der Auftragnehmer ist verpflichtet, bei einer Änderung an den Produkten und/oder bei einer Änderung der gesetzlichen Exportbestimmungen den Auftraggeber darüber unverzüglich zu informieren und die Exportdaten zu aktualisieren.

11.4

Schäden, die dem Auftraggeber durch falsche oder unterlassene Exportangaben entstehen, gehen zu Lasten des Auftragnehmers.

11.5

Der Auftragnehmer wird alle für die Durchführung des Projektvertrages und der jeweiligen Einzelaufträge erforderlichen öffentlich-rechtlichen Bestimmungen einhalten und alle erforderlichen Genehmigungen der zuständigen in- und ausländischen Behörden für die vertraglichen Lieferungen und Leistungen rechtzeitig und auf seine Kosten beantragen.

12 Einsichts-, Prüf- und Kontrollrechte des Auftraggebers (Audits)

12.1

Dem Auftragnehmer ist bekannt, dass der Auftraggeber dem Kunden mitteilt, dass der Auftragnehmer zur Leistungserbringung herangezogen wird. Der Auftragnehmer erklärt sich damit einverstanden, dass auf Verlangen des Kunden / Endkunden diesem diejenigen Auszüge aus diesem Projektvertrag und/oder Einzelauftrag übergeben werden, die erforderlich sind, um die Einhaltung der Bestimmungen des Leistungsvertrages zwischen dem Auftraggeber und dem Kunden/Endkunden überprüfen zu können.

12.2

Der Auftraggeber ist bei konkretem Anlass berechtigt, die Einhaltung der Vertragspflichten durch den Auftragnehmer nach angemessener Vorankündigung in dessen Geschäftsräumen innerhalb der üblichen Geschäftszeiten zu überprüfen. Ein ggf. von dem Auftraggeber in diesem Zusammenhang beauftragter Dritter darf kein Wettbewerber des Auftragnehmers sein und muss entsprechend den Vorschriften dieses Projektvertrages zur Vertraulichkeit verpflichtet werden. Letzteres gilt nicht, sofern der beauftragte Dritte bereits aus gesetzlichen bzw. standesrechtlichen Regelungen zur Vertraulichkeit verpflichtet ist. Ferner sind für die Durchführung der Audits die Sicherheitsbestimmungen der Auftragnehmerin zu beachten, die jedoch zu keinerlei Einschränkungen des vorgenannten Prüfrechts des Auftraggebers führen dürfen.

12.3

Der Auftraggeber ist insbesondere berechtigt, die für den Nachweis der Einhaltung der Vertragspflichten relevanten Unterlagen und Dokumente einzusehen, wobei eine Open Book Prüfung durch den Auftraggeber nicht vorgesehen ist, soweit die Preisprüfungsrechte des Auftraggebers und Endkunden oder anderer Behörden dies nicht erfordern. Der Auftragnehmer wird den Auftraggeber dabei in zumutbarem Umfang unterstützen und ihm die zur Prüfung erforderlichen Auskünfte erteilen.

12.4

Im Fall einer Eignungsleihe wird der Auftragnehmer mit dem Unterauftragnehmer ein entsprechendes Einsichts-, Prüf- und Kontrollrecht zugunsten des Auftraggebers vereinbaren.

12.5

Weitergehende einzelauftragliche Auditrechte des Auftraggebers bleiben unberührt.

13 Verzug

Wird ein zwischen den Parteien vereinbarter Leistungs- oder Liefertermin überschritten, gerät der Aufragnehmer ohne separate Nachfristsetzung durch den Auftraggeber mit sofortiger Wirkung in Verzug, es sei denn, dass die Leistung infolge eines Umstands unterbleibt, den der Auftragnehmer nicht zu vertreten hat. Kommt der Auftragnehmer in Verzug, so ist der Auftraggeber, soweit dies im jeweiligen Einzelauftrag nicht anderweitig vereinbart ist, berechtigt, für jeden angefangenen

Kalendertag der Verzögerung eine Vertragsstrafe in Höhe von 0,2% des Auftragswerts des Einzelauftrags, mit dessen Leistungen der Auftragnehmer in Verzug ist, zu verlangen. Sofern der Auftragnehmer nur mit einem Teil der Leistungen des jeweiligen Einzelauftrags in Verzug ist, berechnet sich die Vertragsstrafe nach dem auf die Teilleistung entfallenden Anteil des Auftragswertes. Mit Auftragswert im Sinne dieser Ziffer ist die Gesamtvergütung gemeint, die der Auftraggeber unter dem jeweiligen Einzelauftrag für die von dem Auftragnehmer zu erbringenden Vertragsleistungen zu entrichten hat. Soweit die Gesamtvergütung des jeweiligen Einzelauftrags bei Abschluss desselben noch nicht feststeht, beläuft sich der Auftragswert auf die maximale Vergütung, welche die Parteien unter dem jeweiligen Einzelauftrag für die Erbringung der Vertragsleistungen vereinbart haben. Insgesamt darf die Summe der aufgrund dieser Regelung zu zahlenden Vertragsstrafe je Einzelauftrag nicht mehr als 5% des Auftragswerts des jeweiligen Einzelauftrags betragen („Maximalvertragsstrafe“). Unterbleibt bei der Annahme der Lieferung, Leistung oder Nacherfüllung ein entsprechender Vorbehalt durch den Auftraggeber, kann die Vertragsstrafe durch den Auftraggeber dennoch später geltend gemacht werden, bei einer werkvertraglichen Leistung jedoch nur bis zur Schlussrechnung. Weitergehende Verzugsansprüche bleiben mit der Maßgabe unberührt, dass die verwirkte Vertragsstrafe auf etwaige Schadensersatzansprüche angerechnet wird.

14 Abnahme

Soweit der Auftragnehmer einzelauftraglich zur Lieferung eines Werkes i.S.d. § 631 BGB als Vertragsleistung verpflichtet ist, vereinbaren die Parteien i.V.m. Ziffer 1.5 des in der Rangfolge diesem Dokument nachrangigen Anhangs zur Leistungsbeschreibung (Anlage 5) folgendes Vorgehen:

14.1

Der Auftragnehmer benachrichtigt den Auftraggeber, sobald die Vertragsleistung fertiggestellt und zur Abnahme bereit ist. Eine Abnahme durch den Auftraggeber setzt eine erfolgreiche Abnahmeprüfung voraus.

14.2

Soweit der Auftraggeber eine gemeinsame Abnahmeprüfung mit dem Auftragnehmer wünscht, kontaktiert dieser den Auftragnehmer nach Erhalt der Benachrichtigung über die Fertigstellung der Vertragsleistung entsprechend dem Einzelauftrag, um mit diesem einen Termin für eine gemeinsame Abnahmeprüfung für die Vertragsleistung zu vereinbaren. Dieser sollte nicht später als zehn (10) Tage nach Benachrichtigung über die Fertigstellung der abzunehmenden Vertragsleistung stattfinden.

14.3

Während der Abnahmeprüfung prüft der Auftraggeber – auf Veranlassung des Auftraggebers mit Unterstützung des Auftragnehmers –, ob die Vertragsleistung alle Abnahmekriterien und Ziele erfüllt, wie sie im Einzelauftrag vereinbart wurden und erstellt – ggf. gemeinsam mit dem Auftragnehmer – einen Abnahmebericht. Festgestellte Mängel sind zu dokumentieren.

14.4

Nach erfolgreicher Abnahmeprüfung wird der Auftraggeber die Abnahme der Vertragsleistung unverzüglich in Textform bestätigen. Sofern der Auftraggeber die Abnahme nicht innerhalb von

zwei (2) Wochen nach erfolgreicher Abnahmeprüfung bestätigt, hat der Auftragnehmer die Möglichkeit dem Auftraggeber in Textform eine einwöchige Nachfrist zur Abgabe der Abnahmeerklärung zu setzen. Sollte der Auftraggeber nicht innerhalb der Nachfrist in Textform Gründe für eine Abnahmeverweigerung darlegen, gilt die Vertragsleistung als abgenommen. Gleiches gilt, wenn der Auftraggeber die Vertragsleistung nach Ablauf der Nachfrist produktiv nutzt.

14.5

Soweit die Parteien während der Abnahmeprüfung Mängel und/oder Abweichungen von den Abnahmekriterien feststellen, wird der Auftragnehmer diese unverzüglich beseitigen und – soweit es sich nicht um unwesentliche Mängel handelt – eine erneute Abnahmeprüfung initiieren. Wegen unwesentlicher Mängel kann die Abnahme nicht verweigert werden.

15 Beendigungsunterstützung

15.1

Der Auftraggeber kann im Falle der Beendigung eines als Dauerschuldverhältnis zu qualifizierenden Einzelauftrags unabhängig des Beendigungsgrundes die Fortführung der Vertragsleistungen für einen angemessenen Übergangszeitraum, maximal jedoch für zwölf (12) Monate, vom Auftragnehmer verlangen. Dieses Verlangen hat der Auftraggeber dem Auftragnehmer mindestens sechs (6) Wochen vor dem Ablauf des jeweiligen Einzelauftrags schriftlich anzuzeigen, wobei im Falle einer außerordentlichen Kündigung diese Vorankündigungsfrist nicht gilt. Sollte der jeweilige Einzelauftrag durch den Auftragnehmer außerordentlich aufgrund eines Zahlungsverzugs des Auftraggebers wirksam gekündigt werden, wird eine Verlängerung nur gegen eine Vorauszahlung der für die Erbringung der Vertragsleistungen geschuldeten Vergütung gewährt. Für die Verlängerung gelten die Bestimmungen dieses Projektvertrages und des jeweiligen Einzelauftrags, einschließlich der Regelungen zur Vergütung, fort und enden mit Ablauf der Verlängerung, ohne dass es einer Kündigung einer der Parteien bedarf.

15.2

Der Auftragnehmer hat auf Verlangen des Auftraggebers ferner angemessene Unterstützungsleistungen zu erbringen, die erforderlich sind, um einen reibungslosen und erfolgreichen Übergang der Vertragsleistungen auf den Auftraggeber oder einen neuen Anbieter zu ermöglichen und somit eine Kontinuität der Leistungserbringung sicherzustellen. Die Bestimmungen dieses Rahmenvertrages und des jeweiligen Einzelauftrags gelten für solche Unterstützungsleistungen fort. Soweit die Übergabe der Vertragsleistungen auf den Auftraggeber bzw. einen neuen Anbieter nicht auf einem Verschulden des Auftragnehmers beruht, ist der Auftragnehmer berechtigt, eine Vergütung für die Unterstützungsleistungen gemäß der im Preisblatt/ Leistungsverzeichnis (Anlage 6) angegebenen Stundensätze zu verlangen.

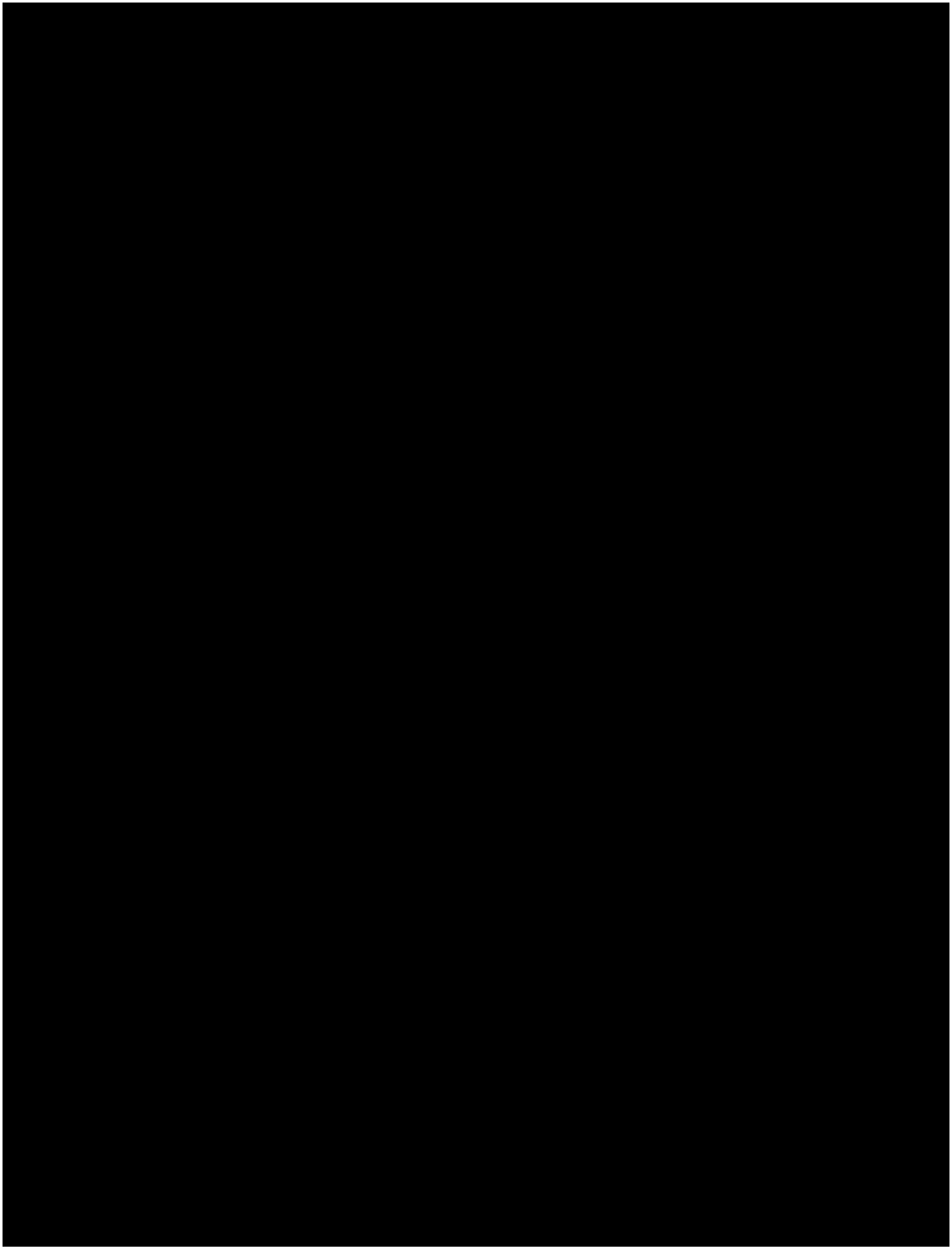
15.3

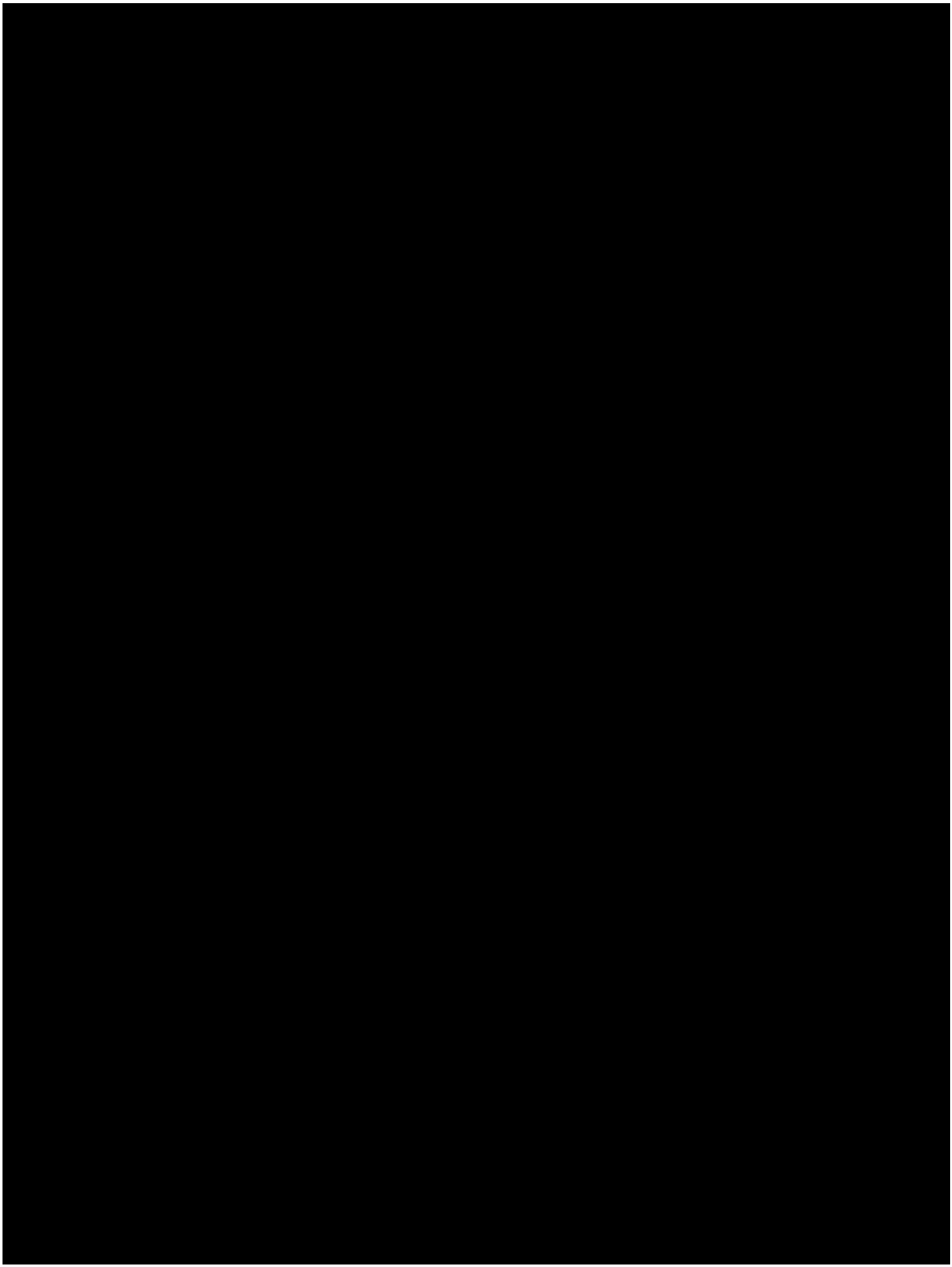
Der Auftragnehmer ist verpflichtet, sämtliche Daten, Dokumente, Aufzeichnungen und sonstigen Informationen, die Bestandteil der Vertragsleistungen sind oder vom Auftraggeber bzw. dem Endkunden zur Erbringung der Vertragsleistungen bereitgestellt worden sind, an den Auftraggeber bzw. den Endkunden unverzüglich mit Beendigung der Vertragsleistungen gleich aus welchem Beendigungsgrund auf einem marküblichen Datenträger herauszugeben bzw. unwiderruflich und datenschutzkonform auf Anforderung des Auftraggebers bzw. des Endkunden zu löschen, soweit dem keine gesetzlichen Aufbewahrungsvorschriften entgegenstehen.

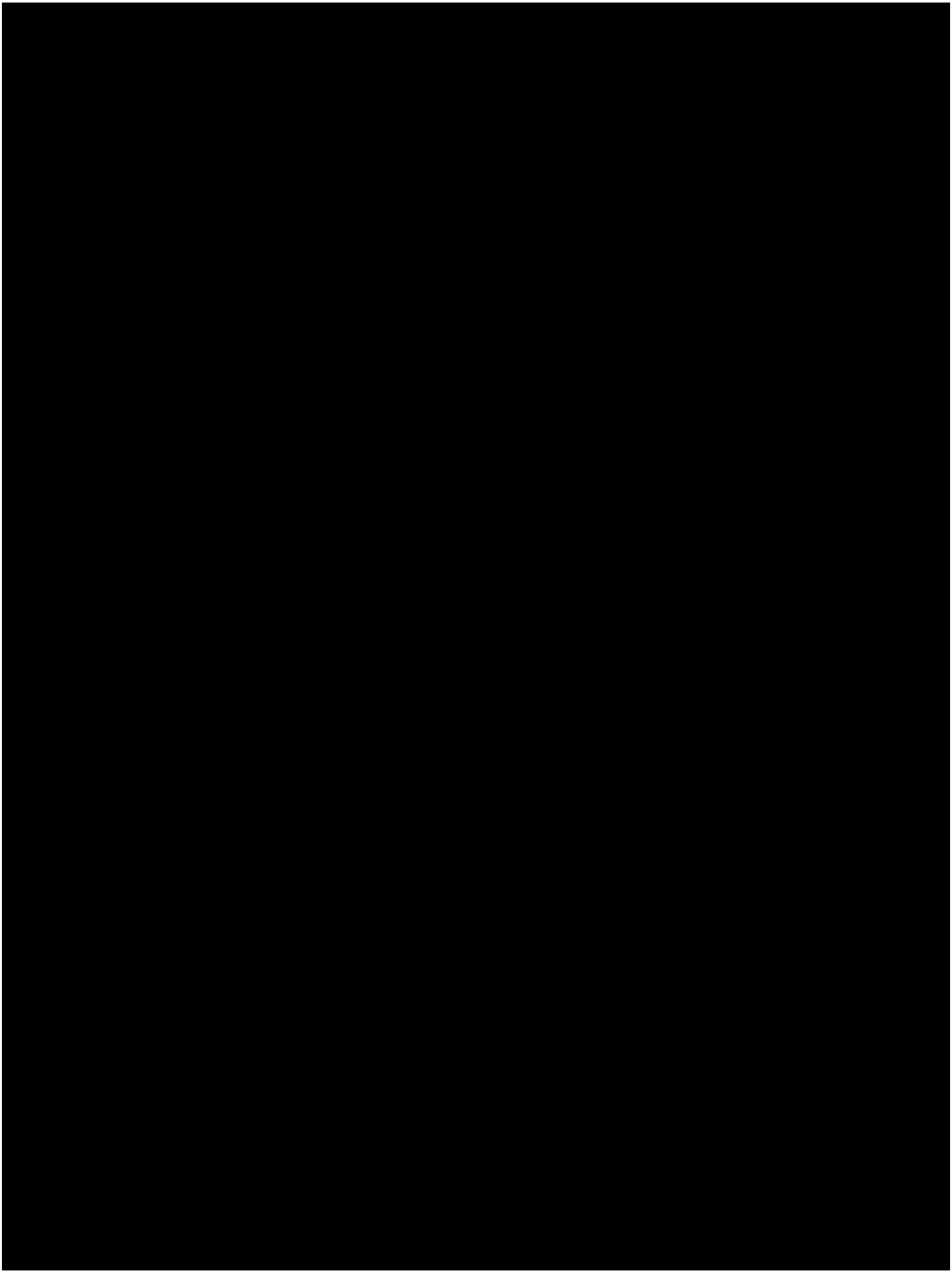
Signatures

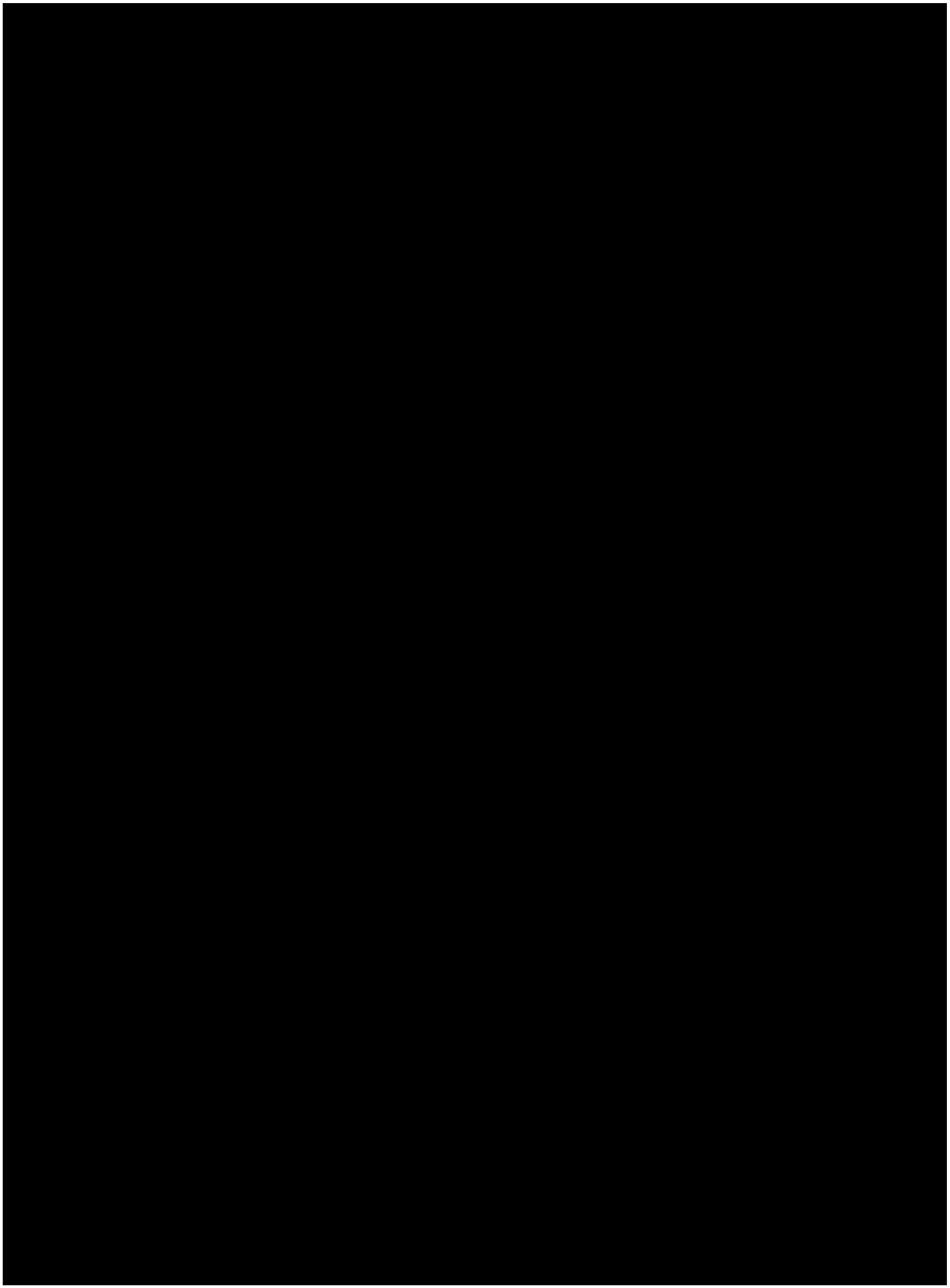
Number of pages (including this one): 19

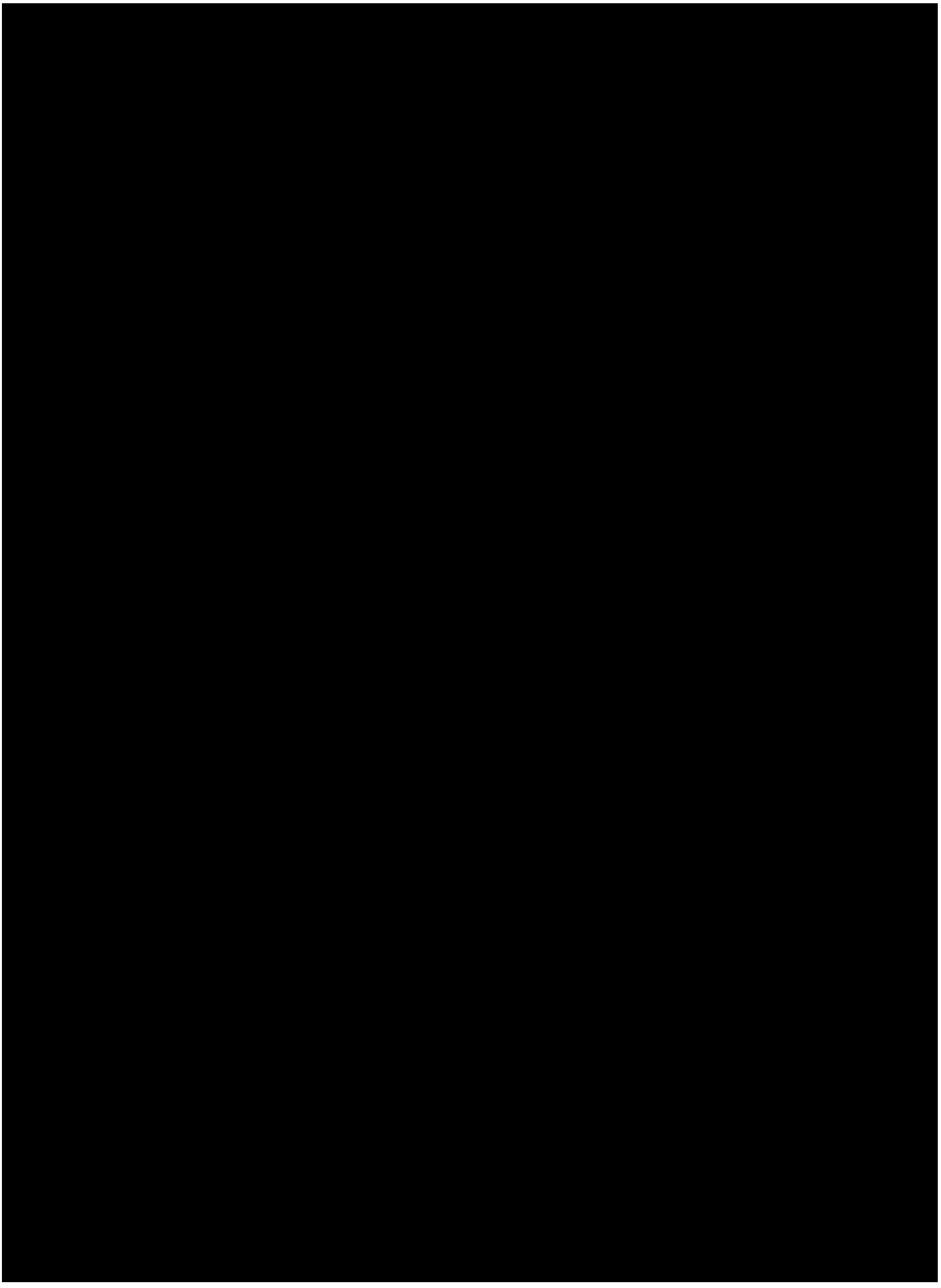
- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.











Signatures

Anlage 3 – Bestellprozess

Bei den nachfolgenden Regelungen handelt es sich um Regelungen aus dem Rahmenvertrag, die auch für die Subunternehmerin Anwendung finden. „Auftraggeber“ ist im Folgenden die T-Systems, „Auftragnehmer“ die Subunternehmerin.

1 Rahmenverträge/ Einzelaufträge

1.1

Im Projektvertrag werden die Bedingungen für Einzelaufträge festgelegt, die während der Vertragslaufzeit abgeschlossen werden können. Eine Abnahmeverpflichtung des Auftraggebers besteht nicht.

1.2

Ein Einzelauftrag kommt zustande, wenn der Auftragnehmer gegenüber dem Auftraggeber die von diesem an den Auftragnehmer in Textform versandte Bestellung innerhalb von vier (4) Arbeitstagen mit einer inhaltlich übereinstimmenden Auftragsbestätigung in Textform annimmt (nachfolgend „Bestellannahmefrist“ genannt), wobei sich die Parteien vor dem Versand einer Bestellung durch den Auftraggeber im Sinne der Regelungen der Ziffer 5 der Leistungsbeschreibung (Anlage 4) vorab abstimmen werden (nachfolgend „abgestimmte Bestellung“ genannt).

1.3

Der Auftragnehmer nur dann berechtigt, eine Bestellung des Auftraggebers auf Basis des Projektvertrages abzulehnen, wenn diesem die Erfüllung der Vertragsleistungen aus der Bestellung des Auftraggebers unmöglich oder unter Abwägung mit dem Leistungsinteresse des Auftraggebers unzumutbar ist und er dem Auftraggeber die Unmöglichkeit oder Unzumutbarkeit innerhalb der Bestellannahmefrist in Textform angezeigt und begründet hat. Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf dessen Verlangen die Unmöglichkeit oder Unzumutbarkeit im Einzelfall nachzuweisen.

1.4

Weicht die Auftragsbestätigung von der betreffenden Bestellung ab, so ist der Auftraggeber an diese Abweichung nur gebunden, soweit er der Abweichung ausdrücklich zugestimmt hat.

1.5

Nach Zustandekommen des Einzelauftrags hat der Auftragnehmer – soweit im Einzelauftrag oder in diesem Projektvertrag nichts Abweichendes geregelt ist - unverzüglich mit der Ausführung der beauftragten Vertragsleistungen zu beginnen.

2 Bestellprozess/ Einzelauftrag

2.1

Bestellungen des Auftraggebers enthalten in Abhängigkeit des jeweiligen Leistungsgegenstands grundsätzlich die folgenden Angaben:

- Bestellreferenz des Auftraggebers

- Bestelldatum
- Bezeichnung(en) und Mengen der bestellten Lieferungen und Leistungen
- Preis pro Bestellposition
- Liefer- und/oder Leistungstermin(e)
- Liefer- und/oder Leistungsort(e)
- Ansprechpartner des Auftraggebers „vor Ort“, also am benannten Liefer-/ Leistungsort und Rechnungsadresse des Auftraggebers

2.2

Der Auftragnehmer hat den Eingang einer jeden Bestellung spätestens am Arbeitstag nach Eingang der Bestellung in Textform dem in der jeweiligen Bestellung benannten „im Einkauf“ verantwortlichen Ansprechpartner des Auftraggebers zusammen mit mindestens den folgenden Angaben zu bestätigen („Bestelleingangsbestätigung“):

- die Bestellnummer des Auftraggebers
- das Bestelldatum

Unter „Arbeitstag“ verstehen die Parteien die Tage von Montag bis Freitag, ausgenommen bundeseinheitliche Feiertage.

2.3

Die verbindliche Auftragsbestätigung des Auftragnehmers im Sinne der Ziffer 1.2 hat die folgenden Angaben aus der Bestellung zu bestätigen:

- die Bestellnummer und das Bestelldatum des Auftraggebers
- Bezeichnung und Menge pro Bestellposition
- Preise pro Bestellposition der betreffenden Bestellung des Auftraggebers
- Gesamtpreis
- der/die Liefer- und/oder Leistungstermin(e)
- der/die Liefer- und Leistungsort(e)
- Ansprechpartner des Auftraggebers „vor Ort“, also am benannten Liefer-/ Leistungsort

2.4

Der Auftragnehmer kann eine Bestellung innerhalb der oben genannten Frist nur dann in Textform zurückweisen, wenn und soweit diese nicht mit den Bestimmungen dieses Projektvertrages übereinstimmt. Ziffer 1.3 dieser Anlage bleibt unberührt.

2.5

Der Auftraggeber ist berechtigt, bis spätestens acht (8) Arbeitstage vor dem Liefer-/ Leistungstermin den Liefer-/ Leistungsort zu ändern und/oder den Liefer-/ Leistungszeitpunkt um bis zu 20 Arbeitstage nach hinten zu verschieben.

2.6

Der Auftraggeber ist berechtigt, Bestellungen nach Zugang einer Auftragsbestätigung zu stornieren. Sollte der Auftraggeber nach diesem Zeitpunkt eine Bestellung stornieren, trägt er die bis dahin beim Auftragnehmer angefallenen Aufwendungen. Die Aufwendungen sind dem Auftraggeber vom Auftragnehmer jeweils nachzuweisen und dürfen in keinem Fall die vereinbarte Vergütung überschreiten. Unberührt bleibt zudem die allgemeine Schadensminderungspflicht des Auftragnehmers.

3 Lieferung, Bereitstellung

3.1

Der Auftragnehmer verpflichtet sich, Vertragsleistungen vollständig und funktionsfähig sowie nach dem Stand der Technik innerhalb des im jeweiligen Einzelauftrag bestimmten Zeitraums (nachfolgend auch „Ausführungsfrist“ genannt) durchzuführen und dem Auftraggeber zur Verfügung zu stellen.

3.2

Zu vorzeitigen Lieferungen und/oder Leistungen sowie nicht vertraglich vereinbarten Teillieferungen/-leistungen ist der Auftragnehmer – vorbehaltlich einer entsprechenden Vereinbarung in den Anlagen oder Anhängen zu diesem Projektvertrag oder im jeweiligen Einzelauftrag – nur mit Zustimmung des Auftraggebers berechtigt.

3.3

Soweit Vertragsleistungen vereinbarungsgemäß bei dem Auftraggeber bzw. den Endkunden vor Ort zu erbringen sind, gelten die nachfolgenden Bestimmungen dieser Ziffer 3.3:

a) Der Auftragnehmer hat bei der Vertragserfüllung die üblichen Geschäftszeiten des Auftraggebers bzw. die üblichen Dienstzeiten der Endkunden zu berücksichtigen.

b) Soweit der Auftragnehmer zur Erbringung der Vertragsleistungen Zugang zu den Standorten des Auftraggebers bzw. Liegenschaften des Endkunden benötigt, hat dieser jeweils die Zutrittsanforderungen und ggf. Hausordnungen des Auftraggebers bzw. Endkunden zu beachten.

Der Auftraggeber wird dem Auftragnehmer die jeweils zu beachtenden Anforderungen rechtzeitig vorab bekannt geben.

3.4

Erkennt der Auftragnehmer, dass er die Vertragsleistungen nicht zu den vereinbarten Terminen bzw. innerhalb der vereinbarten Frist erbringen kann, so hat er dies unter der Angabe der Gründe für die Verzögerung sowie der voraussichtlichen Dauer der Verzögerung unverzüglich dem Auftraggeber mitzuteilen. Etwaige Ansprüche des Auftraggebers aus der nicht fristgemäßen Erfüllung des jeweiligen Einzelauftrags bleiben unberührt. Die vorbehaltslose Annahme der verspäteten Vertragsleistung stellt keinen Verzicht auf die dem Auftraggeber zustehenden gesetzlichen Ansprüche dar.

4 Voraussichtliches Abrufvolumen

Der geschätzte Auftragswert für die unter diesem Projektvertrag zu erbringenden Vertragsleistungen innerhalb der Gesamtvertragslaufzeit von sieben (7) Jahren zzgl. 3-maliger

Verlängerungsoption um jeweils ein (1) Jahr ergibt sich aus dem Preisblatt/ Leistungsverzeichnis (Anlage 6) zu diesem Projektvertrag (siehe „geschätzter Auftragswert“ in der Anlage 6).

Der Auftragnehmer hat jedoch keinerlei Anspruch auf ein bestimmtes Abnahmevolumen.

Signatures

Number of pages (including this one): 5

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

BWI
IT für Deutschland

Leistungsbeschreibung

Anlage 1 zum Rahmenvertrag über den Bezug von Konzeptions- und Entwicklungsleistungen für die „Strategische Partnerschaft pCloudBw“

Inhalt

Inhalt 2
1 Glossar 3
2 Ausgangslage und Zielsetzung 5
3 Leistungsgegenstand 6
4 Leistungskonkretisierung 7
5 Beauftragungsmodelle 22
6 Beistellleistungen und Mitwirkungsobliegenheiten des AG 34
7 Anhänge 35

1 Glossar

Die nachfolgenden Abkürzungen haben die nachstehend definierte Bedeutung und gelten ergänzend zu den im Rahmenvertrag definierten Begriffen, soweit nicht ausdrücklich etwas Anderes vereinbart ist oder sich aus dem Kontext eine andere Bedeutung ergibt.

6R	Gartner Research Application Migration to Cloud
AG	Auftraggeber/ BWI GmbH
AN	Auftragnehmer
BAMAD	Bundesamt für den Militärischen Abschirmdienst
BMVg	Bundesministerium für Verteidigung
BSI	Bundesamt für Sicherheit in der Informationstechnik
Bw	Endkunde Bundeswehr
BwKrhs	Bundeswehrkrankenhaus/-häuser (Berlin, Hamburg, Koblenz, Ulm)
CI/CD	Continuous Integration/ Continuous Delivery
COTS	Commercial of the Shelf
DEUmilSAA	Deutsche militärische Security Accreditation Authority
DoD	Definition of Done.
DoR	Definition of Ready
EPDF	Enterprise Development Frameworks der BWIdes AG
FCAS	Future Combat Air System
Fü(W)ES	Führungs-, Waffen- und Einsatzsysteme
GB	Geschäftsbereich
GesVers	Gesundheitsversorgung
GMN	German Mission Network
HW	Hardware
IaaS	Infrastructure as a Service
IT-SysBw	IT-Systeme der Bundeswehr
NATO	North Atlantic Treaty Organization

OS	Operating System
PaaS	Plattform as a Service
pCloudBw	Private Cloud Bundeswehr
PM(O)	Projekt Management (Office)
POC	Proof of Concept
PoT	Proof of Technology
SaaS	Software as a Service
SAFe	Scaled Agile Framework
SBOM	Secure Software Supply Chain
Secure Assembly Site	Mittels Verschlusssachenanweisung definierte sichere Infrastruktur zum Zusammenbau von Soft- und Hardwarekomponenten zur Ausprägung von pCloudBw Instanzen, insbesondere für den Ansatz höher VS-NfD
SEFBw	Service Entwicklungs Frameworks der Bundes
SouvAPBw	Souveräner Arbeitsplatz Bundeswehr
STA	Strategic Technnology Advisory
SW	Software
VSA	Verschlusssachenanweisung
VS-nfD	Verschlusssache nur für den Dienstgebrauch
Werktag	Montag – Freitag ausgenommen bundeseinheitliche Feiertage

2 Ausgangslage und Zielsetzung

2.1 Ausgangssituation für die Beschaffung

Im Rahmen des Projektes „pCloudBw“ verfolgt die Bw das Ziel, durch den AG eine private Cloud Infrastruktur planen und umsetzen zu lassen, welche die zukünftige Basis für den Betrieb von IT-Systemen für die Bw bilden wird. Dadurch wird die Bw-IT funktional modernisiert und flexibilisiert. Die benötigte Hardware- / Softwareplattform ist zu konzipieren und in der Systemumgebung des IT-SysBw bereitzustellen.

Der AG beabsichtigt daher mit einem zuverlässigen IT-Partner einen Rahmenvertrag über die Konzeption und die Serviceentwicklung der zentralen Sicherheitsarchitektur für die Absicherung von Sicherheitsdomänen VS-NfD und höher (u.a. NATO SECRET, EU SECRET) der pCloudBw als zentrale IT-Lösungsarchitektur des IT-SysBw in unterschiedlichen Bewegungsdimensionen (stationär, verlegefähig sowie mobil), die notwendige Integration (technisch, betrieblich und organisatorisch) in die Gesamtarchitektur der pCloudBw, sowie die mittels der pCloudBw zu erbringenden Services zu schließen. In diesem Zusammenhang stehen die hier gegenständlichen Vertragsleistungen, die zur Konzeption, Umsetzung, Integration sowie Betriebsumsetzung, insbesondere zur Sicherstellung eines ganzheitlichen Ansatzes zur IT-Sicherheit, zur Cyber-Sicherheit und zur Reduzierung der Kenntnismöglichkeit Dritter über die Sicherheitsmechanismen, die die Bw zur Absicherung des IT-SysBw etabliert, benötigt werden.

3 Leistungsgegenstand

Die vom AN unter diesem Rahmenvertrag zu erbringenden Vertragsleistungen bestehen gegenständlich aus den folgend aufgeführten Leistungspaketen, die in der nachfolgenden Ziffer 4 jeweils konkretisiert werden.

Leistungspaket	
A	Leistungspaket A - Zentrale Sicherheitsarchitektur
B	Leistungspaket B - Migration / Integration von Services
C	Leistungspaket C - Multi-Cloud
D	Leistungspaket D - Agile Transformation
E	Leistungspaket E - Projektmanagement Aufbau pCloudBw
F	Leistungspaket F - Betrieb neuer IaaS-Stack
G	Leistungspaket G - DevSecOps Betrieb und Weiterentwicklung pCloudBw
H	Leistungspaket H - Konzeption, Realisierung und Betrieb sowie Betriebssupport einer Cloud native Open Source Suite
I	Leistungspaket I - Aufbau Application (SaaS-) Stack

4 Leistungskonkretisierung

Die vom AN auf Basis eines entsprechenden Einzelauftrags bzw. mehrerer Einzelaufträge unter diesem Rahmenvertrag zu erbringenden Vertragsleistungen beinhalten die nachfolgend aufgeführten Leistungspakete mit den im jeweiligen Einzelauftrag konkretisierten Leistungsinhalten und Arbeitsergebnissen. Die konkrete Spezifizierung der vom AN innerhalb eines Leistungspakets zu erbringenden Vertragsleistung erfolgt durch den AG folglich auf Einzelauftragsbasis.

Der AG ist jederzeit berechtigt, auch nur Teile der nachfolgend beschriebenen Leistungspakete beim AN durch Abschluss eines Einzelauftrags unter diesem Rahmenvertrag zu beauftragen.

Die vom AN unter diesem Rahmenvertrag auf Basis eines Einzelauftrags zu erbringenden Vertragsleistungen können nach Veranlassung und Ausgestaltung des AG ganz oder teilweise sowohl als Dienst- als auch als Werkleistungen beauftragt werden (vgl. auch Ziffer 5 dieser Anlage 1 (Beauftragungsmodelle)).

Soweit im jeweiligen Einzelauftrag nichts Abweichendes vereinbart ist, findet die im **Anhang** (Verbindliche Anforderungen aus der Projektmanagement-Systematik der BWI GmbH) zu dieser Leistungsbeschreibung vereinbarte Projektmanagementmethode Anwendung, die auf Veranlassung des AG im jeweiligen Einzelauftrag ausdifferenziert wird.

Aus Gründen der besseren Lesbarkeit wird in dieser Leistungsbeschreibung das generische Maskulinum verwendet. Gemeint sind jedoch immer alle Geschlechter.

4.1 Leistungspaket A - Unterstützung Customer Solution STA

Der AN hat mit Abschluss eines oder mehrerer leistungskonkretisierender Einzelaufträge unter diesem Rahmenvertrag im Leistungspaket „Unterstützung Customer Solution STA“ insbesondere folgende Vertragsleistungen zu erbringen:

- Leistungen zur Ableitung und Definition von zentralen Sicherheitskomponenten für die pCloudBw
- Leistungen zur Ableitung und Definition von Anforderungen an Systemkomponenten der pCloudBw, insbesondere vor dem Hintergrund der IT-Sicherheit, aus national und international gültigen Vorgabendokumenten (NATO, EU, BSI, Bw etc.)
- Evaluierung/ Marktanalyse vorhandener Teilkomponenten/ Alternativen (COTS), um auf einem Demonstrator konkrete Szenarien durchzuführen
- Leistungen zur Ableitung, Definition und Umsetzung einer Secure Assembly Site
- Leistungen zur Ableitung, Definition und Umsetzung von Elementen zu Prüfung von Cloudsoftware unter Einhaltung der Vorgaben der VSA für den Ansatz höher VS-NfD sowie vergleichbarer NATO und EU Vorgaben
- Leistungen zur Ableitung, Definition und Umsetzung von Test-, Integrations- und Entwicklungsumgebung für die pCloudBw
- Leistungen zur Evaluierung von cloudspezifischen Lösungen und Fähigkeiten auf Basis der Test-, Integrations- und Entwicklungsumgebung für die pCloudBw, unter Einbezug von Dritten (u.a. deutsche Rüstungsunternehmen, NATO)

- Leistungen zur Ableitung, Definition und Umsetzung von Zulassungsverfahren für Soft- und Hardwarekomponenten im Cloudumfeld. Hierzu zählt die Dokumentation.
- Leistungen zur Ableitung, Definition und Umsetzung in Bezug auf Marktanalyse von für die pCloudBw erforderlichen Soft- und Hardwarekomponenten
- Leistungen im Rahmen von Pentesting für pCloudBw Anteile in IaaS, Paas und SaaS – Layer und deren Dokumentation
- Leistungen zur Ableitung, Definition und Umsetzung von Service Tests, sowie bei der Vorbereitung des Service Deployments und ggf. Migration
- Leistungen zur Ableitung, Definition und Umsetzung von Cloud-Securityprozessen
- Leistungen zur Ableitung, Definition und Umsetzung in Bezug auf Betriebsunterstützung von Rechenzentrumsumgebung. Hierzu zählt der Aufbau und Betreuung der Betriebsplattform über den IT-Lifecycle und die Umsetzung von Infrastructure as Code auf Basis der Modelle
- Leistungen zur Ableitung, Definition und Umsetzung von Modellierungen und Modellanpassung unter Anwendung der Architekturmethode der Bw und der Notation NAFv4-ADMBw bei Modellierungen von operationellen Architekturen und Servicearchitekturen unter Bedienung des Modellierungswerkzeug Sparx EA v16. Hierzu zählt die Initiierung, Erarbeitung und Qualitätssicherung von Architekturen sowie Planung und Durchführung von Präsenz/ Remote Aus-/ Weiterbildungen im Bezug auf das Modellieren nach NAFv4-ADMBw
- Leistungen zur Ableitung, Definition und Umsetzung von Requirement Engineering nach IREB unter Verwendung von Require.7 und/ oder IBM Doors entlang des IT-Lifecycle
- Leistungen zur Definition und Umsetzung und Weiterentwicklung einer bereits modellierten Methode, mit welcher sich der Nachweis führen lässt, dass ein System gegen Angriffe geschützt ist

4.2 Leistungspaket B – Migration / Integration von Services

Der AN hat mit Abschluss eines oder mehrerer leistungskonkretisierender Einzelaufträge unter diesem Rahmenvertrag im Leistungspaket „Migration / Integration von Services“ insbesondere folgende Vertragsleistungen zu erbringen:

- Service Assessment / Ausplanung / Priorisierung im Context Bw und AG
- Analyse der Cloud-Eignung und Ausplanung der Services und Solutions inkl. schützenswerter HW- und SW Komponenten und derer Abhängigkeiten entsprechend der VS-NfD Klassifizierung. Die Basis für Analysen bilden Bestandsdaten und Ergebnisse (Interview basierte) der Assessments
- Auswertung, Aufplanung und Priorisierung der Migration von Services auf Basis einer Migrationsplanung (-Roadmap)
- Durchführung eines Migration Discovery sowie eine Abhängigkeitsanalyse (Tool gestützt)
- Customizing / Implementierung / Rollout / Betrieb eines (toolgestützten) Verfahrens zur Analyse der Services und Solutions mit schützenswerten HW- und SW Komponenten (VS-NfD und höher eingestuft) und deren Abhängigkeiten

- Aufnahme, Auswertung und Vorbereitung der erhobenen Daten für die Migrationsplanung
- Die zur Automatisierung und Optimierung von Abläufen der Migration vorgesehene Tool gestützte Applikation, welche nach einer entsprechenden Marktanalyse zur Auswahl steht, wird auf ihre Einsatzfähigkeit technologisch im Rahmen eines PoT´s bewertet. Im Rahmen dieses Vorgangs müssen im Vorfeld die Requirements beschrieben und gewichtet werden. Die Ergebnisse eines PoT´s werden dann eines Scorings unterzogen und in eine Entscheidungsvorlage überführt.
- Für die Beantragung von Stützservices ist ein Architekturdiagramm zu erstellen. Vorgaben / Templates werden vom AG bereitgestellt. In diesem Architektur Diagramm ist zudem herauszuarbeiten, ob der jeweilige Service BiModal oder auf bestehende Stützservices aufsetzt.
- Leistungen zu Migrations- und Integrationsvorhaben von Applikationen, welche potentiell auf die Zielplattformen transformiert werden. Das Verfahren und die Methodik sind von der Einheit “Cloud Migration” des AG vorgegeben.
- Gemäß Strategie des AG sind Applikationen containerisiert bereitzustellen. Ein entsprechender Transformationsweg ist technologisch für das jeweilige Vorhaben (Applikation) technisch zu entwickeln und nach dem DevSecOps Modell umzusetzen. Die Betriebsfähigkeit ist in der jeweiligen Zuständigkeit (Bw/AG) sicherzustellen.
- Begleitung eines Onboardings (Legitimation von Berechtigungen etc) der Entwickler und Betriebseinheiten auf die Cloud.
- Unterstützung in der Entwicklung von Applikationen in einem VS, inkl VS-NfD und höheren Zieldesign. Eine entsprechende Transformationsplanung ist zu erstellen.
- Planung und Vorbereitung der Implementierung von sicherheitskritischen Services und Solutions
- Durchführung von Requirement Engineering Management inkl. Abstimmung von Portfolio und Cloud Roadmap
- Aufnahme von Anforderungen der Services und Solutions VS-NfD oder höher an die Cloud Services und Funktionen
- Abgleich mit der Cloud und Portfolio Roadmap
- Leistungen zur Kopplung von Rechenzentren und Plattformen im Context “Netzwerkservices” mit der Zielsetzung den jeweiligen Workload transferieren und integrieren zu können
- Überführen von Daten (DataBase) von einem zu tranfomierenden Datenbanksystem. In diesem Handlungsfeld sind entsprechende Konzepte zu entwickeln.
- Sofern sich im Rahmen der Transformation von Applikationen nach dem 6 R Verfahren auch Anpassungen am Sicherheitskonzept pCloudBw ergeben, sind diese entsprechend aufzuzeigen und dem Bereich CISO des AG zu übermitteln.

4.3 Leistungspaket C - Multi-Cloud

Der AN hat mit Abschluss eines oder mehrerer leistungskonkretisierender Einzelaufträge unter diesem Rahmenvertrag im Leistungspaket „Multi-Cloud“ insbesondere folgende Vertragsleistungen zu erbringen:

- Ableitung einer Multi-Cloud Strategie und Entwurf einer Multi-Cloud Management Architektur (ggf. mit Markterkundung und PoC)
- Customizing / Implementierung / Rollout / Betrieb eines (toolgestützten) Verfahrens zur Analyse der Services und Solutions mit schützenswerten HW- und SW-Komponenten (VS-NfD und höher eingestuft) und deren Abhängigkeiten
- Für die Beantragung von Stützservices ist ein Architekturdiagramm zu erstellen. Vorgaben / Templates werden vom AG bereitgestellt. In diesem Architektur Diagramm ist zu dem herauszuarbeiten, ob der jeweilige Service BiModal oder auf bestehende Stützservices aufsetzt.
- Erstellung von Lösungs- und Servicekonzepten entsprechend Service Entwicklungs Framework (SEFBw und EPDF) des AG
- Sicherstellen der fachbereichsübergreifenden Konsistenz und Durchgängigkeit der Solution / des Service (End to End)
- Inhaltliche Abstimmung, Beschreibung und Einholung von Freigaben in Bezug auf die Anforderungen des jeweiligen Auftraggebers (Portfoliomanagement / Demandmanagement)
- Inhaltliche Abstimmung, Beschreibung und Einholung von Freigaben in Bezug auf Lösungs- und Servicekonzepte mit den Betriebseinheiten und deren Service Architekten.
- Betriebsunterstützung Multi-Cloud
    - Integrationstests: Durchführung umfassender Integrationstests zur Sicherstellung sowohl der Stabilität und Integrität der Plattform als auch Kompatibilität mit den verwalteten (Multi-) Cloud-Ressourcen und -Diensten
    - Kontinuierliche Wartung und Aktualisierung: Regelmäßige Updates und Patches für alle integrierten Plattform Komponenten (HW+SW)
    - Überwachung und Monitoring: Überwachung von Performance und Stabilität der Plattform. Grundlage dafür ist das kontinuierliche Monitoring der Systems, sowie die Sammlung von Logs und deren Analyse und die Darstellung bzw. das Reporting mit Hilfe von entsprechenden Dashboards.
    - Sicherheitsmanagement: Regelmäßige Sicherheitsüberprüfungen, Schwachstellenmanagement, Durchführung von Schwachstellen-Scans und Penetrationstests und Implementierung von Sicherheits- und Auditmaßnahmen zum Schutz der Plattform. Dazu gehört u.a. eine Richtlinienverwaltung, Vault für Geheimnisverwaltung und verschiedene Tools zur Einhaltung von Compliance-Anforderungen sowie Netzwerkmanagement und Netzwerksicherheit.
    - Skalierbarkeit: Sicherstellung der Skalierbarkeit der Plattform zur Unterstützung wachsender Anforderungen und Nutzerzahlen
    - Fehlerbehebung und Support: Aufbau und kontinuierliche Weiterentwicklung von Incident Response Plänen für die Durchführung von Incident Management und die Bereitstellung eines 24/7-Supports zur schnellen Behebung von Problemen und zur Unterstützung der Nutzer
    - Automatisierung: Einsatz von Automatisierungstools zur Optimierung von Betriebsabläufen, Bereitstellungsprozessen, Konfigurationsmanagement und CI/CD-Pipelines zur Reduzierung manueller Eingriffe
    - Dokumentation: Kontinuierliche Erstellung, Weiterentwicklung und Pflege umfassender Dokumentation für alle Komponenten und Prozesse der Plattform
    - Kostenmanagement: Implementierung von Tools zur Überwachung und Optimierung der Betriebskosten. Dies schließt explizit die verwalteten (Multi-) Cloud-Ressourcen und –Dienste ein.

- Compliance und Governance: Sicherstellung der Einhaltung aller im Rahmen der Erbringung der Vertragsleistungen relevanten gesetzlichen und regulatorischen Anforderungen

- Ableitung eines Lösungsansatzes und eines Service-Schnitts.
- Fachliche/inhaltliche Erstellung des Solution Designs, der Leistungsbeschreibung, der Kostenkalkulation und weiterer Kunden- bzw. Projektspezifischer Dokumente.
- Ableitung und Durchführung von Solution Tests, sowie bei der Vorbereitung des Solution Deployments und ggf. Migration.
- Die zur Automatisierung und Optimierung von Abläufen der Migration vorgesehene Tool gestützte Applikation, welche nach einer entsprechenden Marktanalyse zur Auswahl steht, wird auf ihre Einsatzfähigkeit technologisch im Rahmen eines PoT´s bewertet. Im Rahmen dieses Vorgangs müssen im Vorfeld die Requirements beschrieben und gewichtet werden. Die Ergebnisse eines PoT´s werden dann eines Scorings unterzogen und in eine Entscheidungsvorlage überführt.
- Leistungen zur Kopplung von Rechenzentren und Plattformen im Context “Netzwerkservices” mit der Zielsetzung, den jeweiligen Workload transferieren und integrieren zu können.

4.4 Leistungspaket D - Agile Transformation

Der AN hat mit Abschluss eines oder mehrerer leistungskonkretisierender Einzelaufträge unter diesem Rahmenvertrag m Leistungspaket „Agile Transformation“ insbesondere folgende Vertragsleistungen zu erbringen:

- Ableitung eines agilen Betriebsmodells pCloudBw unter Berücksichtigung der relevanten Schnittstellen innerhalb des AG
- Coaching agiler Methoden in einem skalierten agilen Umfeld Konzepterstellung
- Schulung von Mitarbeitern des AG in den agilen Methodiken und Praktiken
- Umsetzung und Einhaltung der agilen Arbeitsweise in den agilen Teams
- Moderation und Führung der agilen Zeremonien in den agilen Teams und in skalierten Frameworks
- Integration des agilen Betriebsmodells pCloudBw in die Bestandsprozesse des AG
- Implementierung des agilen Betriebsmodells der Cloud-Plattformen
- Aufstellung und Weiterentwicklung des agilen Betriebsmodells
- Weiterentwicklung des DevOps Modells hin zu einem DevSecOps Modell

4.5 Leistungspaket E - Projektmanagement Aufbau pCloudBw

Der AN hat mit Abschluss eines oder mehrerer leistungskonkretisierender Einzelaufträge unter diesem Rahmenvertrag im Leistungspaket „Projektmanagement Aufbau pCloudBw“ insbesondere folgende Vertragsleistungen zu erbringen:

- Steuerung, Implementierung und Weiterentwicklung des hybriden Projektmanagement-Ansatzes im Kontext der pCloudBw in Anlehnung an das AG-interne PM-Framework “PM@BWI" (siehe Anhang) und an agile Frameworks wie bspw. Scrum, SAFe und Kanban

- Auswahl, Entwicklung und Anpassung des Projektmanagementansatzes / Projektdesigns zur bestmöglichen Erfüllung der Projektziele und Erfolgskriterien anhand der Projektkomplexität
- Lessons Learned aus anderen Projekten überprüfen, anwenden und austauschen
- Erstellung von (Projekt-) Fortschritts-/Zeitplänen sowie Steuerung, Monitoring und Tracking der damit verbundenen Arbeitspakete und Projektaktivitäten
    - Management der (Zeit-) Meilensteine im klassischen PM-Kontext
    - Erstellung und Begleitung von Releaseplänen, Roadmaps und (Program-) Forecast im agilen Kontext
    - (Projekt-) Management von einzelnen PM-Aktivitäten in Form von agilen Items wie bspw. Epics, UserStories oder Tasks und klassischen Arbeitspaketen (u.a. Wasserfall-Modell, Entwicklung im EPDF & SEFBw Framework)
    - Management von Scope, Lieferobjekten und Abhängigkeiten
    - Identifikation, Aufbereitung und Prozessierung erforderlicher (vertraglicher) Projekt-Changes

- Abbildung des Projektkostenmanagements
    - Erstellung von Soll-/Ist-Analysen, Impact-Analysen, Forecast-Berichten und projektbezogenen Reports
    - Allgemeine Budgetverfolgung und –kontrolle
    - Aufbereitung, Analyse und Bewertung von KPIs / Kennzahlen zur Feststellung des Mittelverbrauchs sowie Ableitung entsprechender (Gegen-) Maßnahmen zur Sicherung der Projektvorgaben
    - Erstellung und Management einer Projekt-Personalplanung im Rahmen des Projekt-Budgets
    - Steuerung und Controlling von Leistungen anderer Lieferanten des AG

- Abbildung des (Projekt-) Ressourcen- und Kapazitätsmanagements
    - Planung, Steuerung und Akquise von Personalressourcen in unterschiedlichen Projektvorhaben
    - Zusammenstellung, Steuerung und Entwicklung von Projektteams
    - Konfliktmanagement und Krisenmanagement
    - Steuerung von Projektteams in einer Matrix-Organisation
    - Steuerung des Projektmanagement Office
    - Steuerung und Weiterentwicklung der Fähigkeiten der Projektmitarbeiter im agilen und klassischen Kontext
    - Sicherstellung der Einhaltung der Compliance Regeln, Kultur und Werte des AG
    - Steuerung und Nachverfolgung der Arbeitsergebnisse der Projektmitarbeiter
    - Erstellung von Leistungsbeschreibungen für die Zulieferungen von festen Arbeitspaketen durch Lieferanten

- Vorbereitung, Teilnahme und Moderation an/von Workshops und (Projekt-)Gremien wie bspw. Steuerungs-/Leitungskreisen, Management-Spaces, etc.
    - Übernahme des Stakeholdermanagements
    - Kommunikations-/Moderationsfunktion
    - Verhandlung von Arbeitsergebnissen, Prioritäten und Leistungen des Projekts
    - Entwicklung von Optionen und Alternativen zur Erreichung der Projektziele

- Übernahme von Aktivitäten im Kontext Projekt-/Risikomanagement
    - Formulierung, Qualifizierung und Tracking von Projektrisiken

- Ableitung und Implementierung von (Gegen-) Maßnahmen zur Begegnung von Projektrisiken (u.a. Minimierung, Mitigation)
- Identifikation und Tracking von Projektabhängigkeiten (Abhängigkeitsmanagement) sowie den daraus resultierenden, möglichen Risiken und Problemen

- Kontinuierliche Erstellung und Pflege von Projektdokumentationen wie bspw. Projektstatus-/Fortschrittsberichte, Zeitpläne, Kosten- und Leistungsübersichten, Qualitätspläne, Abnahmedokumentation, Lessons Learned Dokumentation etc.
- Unterstützungsleistungen bei der Anfertigung von projekt-/themenbezogenen Konzepten und Arbeitspapieren im Kontext von Cloud-/Multi-Cloud-Lösungen (bspw. Lasten-/Pflichtenhefte, Anforderungskonzepte, Sicherheitskonzepte, Architekturkonzepte)
- Unterstützungsleistungen im Zusammenhang mit der Projekt-Kommunikation

4.6 Leistungspaket F - Betrieb neuer IaaS-Stack

Der AN hat mit Abschluss eines oder mehrerer leistungskonkretisierender Einzelaufträge unter diesem Rahmenvertrag im Leistungspaket „Betrieb neuer IaaS Stack“ insbesondere folgende Vertragsleistungen zu erbringen:

- Betriebs- und Supportleistungen IaaS-Stack (L2-Betrieb)
  - Netzwerk
    - Implementieren von Netzwerk Solutions, um den IaaS-Stack in einer selbst-gemanagten Umgebung zu supporten.
    - Erkennen und Lösen von Netzwerkproblemen.
    - Unterstützen im Kundensupport
  - Kubernetes
  - Virtualisierung
  - Istio
  - PKI
  - Linux
    - Troubleshooting & Lösen von Problemen im Linux Umfeld
  - Windows Basics (AD, Hyper-V GDC, GPOs) und Windows Advanced (Desired State Configuration, Config Manager, PowerShell)
  - Ansible
  - Prometheus
  - Backup und Recovery
  - Administration von Berechtigungen
  - Monitoring
- Leistungen zum Lifecycle Management des IaaS-Stack (Prüfung und Durchführung von Software Updates)
- Aufbau und Installation des IaaS Stack (VS-NfD bis GEHEIM)
  - Aufbau Hardware (Rz-Operation)
  - Installation und Konfiguration IaaS Stack
- Leistungen zur Implementierung, Integration und Betrieb von PaaS
- Leistungen zur Vorbereitung und Durchführung der Integration des IaaS Stacks in IT-SysBw (VS-NfD bis GEHEIM)
- Leistungen zur Konzeption der Architektur und des Solution Design
- Vorbereitung und Durchführung der Akkreditierung VS-NfD des IaaS-Stack

- Ableitung und Bewertung der Sicherheitsstandards
- Leistungen zur Erstellung des Sicherheitskonzeptes
- Integration in die zentrale Sicherheitsarchitektur pCloudBw
- Leistungen zur ganzheitlichen Service-Entwicklung nach EPDF und SEFBw
- Leistungen zur Erstellung des Betriebsmodells und -konzepts
- Leistungen zur Zulassung von erforderlichen technischen Komponenten
- Modellierungen nach NAFv4
- Leistungen zur Durchführung des Testing
- Leistungen zur Anforderungsanalyse
- Leistungen zum Capacity- und Demand-Management
  - Abruf von Infrastruktur und Ressourcen
- Leistungen zur Analyse, Integration und Onboarding von Workloads auf den IaaS Stacks

4.7 Leistungspaket G - DevSecOps Betrieb und Weiterentwicklung pCloudBw

Der AN hat mit Abschluss eines oder mehrerer leistungskonkretisierender Einzelaufträge unter diesem Rahmenvertrag im Leistungspaket „DevSecOps Betrieb und Weiterentwicklung pCloudBw“ insbesondere folgende Vertragsleistungen zu erbringen:

- Leistungen zur Erstellung eines Betriebsmodells für die SAP Private Cloud
- Leistungen zur Integration von SAP Private Cloud in IT-SysBw (u.a. IAM, SIEM)
- Leistungen im Rahmen von Betrieb und Support der SAP Platform, u.a.
  - Backup und Recovery
  - Administration von Berechtigungen
  - Monitoring
  - Service Request Management
  - Einbringen von Know-How zu Cloud-Technologien:
    - Erfahrung mit den führenden Cloud-Plattformen (z.B. AWS, Microsoft Azure, Google Cloud) und deren Integration mit SAP-Systemen.
    - Weitere Skills (Linux, Helm, Bash Scripting, Container Technologien wie Docker, Kubernetes)
  - Netzwerk und Sicherheit:
    - Verständnis der Netzwerkkonfiguration und Sicherheitsanforderungen in Cloud-Umgebungen, einschließlich VPN, Firewalls und IAM
  - SAP spezifische Inhalte zu Business Technology Platform (BTP)
    - Erfahrung mit Produkten wie Cloud Foundry, Gardener, Terraform, Github / GitLab, HashiCorp Vault, HANA Cloud
    - OCM-CLI (Open Component Model)
    - Stützservices (IAM, PKI und co.)
    - CI/CD
    - Installation / Deployment / Automatisierung
- Leistungen zum ganzheitlichen Lifecycle Management der SAP Private Cloud (u.a. Prüfung und Durchführung von Software Updates)
- Installation und Konfiguration der SAP Private Cloud
- Leistungen zur Konzeption der Architektur und des Solution Design
- Ableitung und Bewertung der Sicherheitsstandards
- Leistungen zur Erstellung des Sicherheitskonzeptes

- Leistungen im Rahmen der ganzheitlichen Service-Entwicklung nach EPDF und SEFBw.
- Modellierungen nach NAFv4
- Leistungen zur Durchführung des Testing
- Leistungen im Rahmen der Anforderungsanalyse
- Leistungen beim Capacity- und Demand-Management
- Leistungen im Rahmen der Analyse, Integration und Onboarding von Workloads auf die SAP Private Cloud

Folgende Leistungen sind in Form von Konzeption, Entwicklung, PoCs, Implementierung und der Übernahme bzw. Unterstützung des Betriebs der zentralen Sicherheitsarchitektur sowie deren Integration in alle auf der pCloudBw abgebildeten Services zu erbringen:

- Betrieb und Weiterentwicklung der Containerplattform
- Betrieb und Weiterentwicklung der Virtualisierungsplattform
- Betrieb und Weiterentwicklung des Datenbankservices
- Betrieb und Weiterentwicklung der Plattform für Geo-Informations-Systeme
- Betrieb und Weiterentwicklung des Storagesystems (File-/Objectstorage)
- Betrieb und Weiterentwicklung des ManagedOS
- Betrieb und Weiterentwicklung der CRSI Rack Architektur & Interimslösung

Darüber hinaus sind die folgenden Leistungen zu erbringen:

- Prozessentwicklung / Prozessmodellierung
  - Festlegung servicespezifischer Anwendungsfälle nach Vorgabe der Geschäftsarchitektur des AG sowie Definition, Planung und Entwicklung servicespezifischer Prozesse, Prozessrollen und Arbeitsplänen
  - Erarbeitung und Präsentation möglicher Prozessablaufoptimierung
  - Dokumentation der prozessualen Aufgaben sowie der Ergebnisse der Serviceimplementierung anhand des Dokumentationsframeworks des AG
- Produktentwicklung
  - Weiterentwicklung für das Cloud-basierte Produktmanagement nach ITSM-Vorgaben
  - Entwicklung und Fortschreibung des Cloud-Zielbildes auf Basis der übergeordneten Vision und der Strategischen Ziele des Unternehmens sowie Anbindung an OnPremise (bestehende) Systeme
  - Aufbau, Pflege und kontinuierliche Qualitätssicherung der Release Roadmap
  - Aufbau Demand Management und Schnittstelle zum Kunden
  - Entwicklung von Produkten und Services aus den Vorgaben der Programmplanung
    - Konzeption der Cloudprodukte nach ITSM-Vorgaben
    - Konzeption von Konnektoren zur bestehenden IT-Landschaft
    - Konzeption zur Integration in die Cloud Management System
- Entwicklung eines Abrechnungsmodells
  - Kostenermittlung und –abbildung für die Bereitstellung der pCloudBw sowie Auflistung aller (geplanten) Cloud Services gemäß Serviceschnitt
  - Stakeholdergerechtes Aufbereiten der Informationen aus der Katalogisierung
  - Erstellung von Dashboards gemäß Vorgabe des AG im BI-Tool

- Anwendung eines marktüblichen Verrechnungmodells unter Berücksichtigung der ermittelten Kosten
- Erstellen eines PoC für das Verrechnungsmodell nach Vorgaben der des AG
- Implementierung des Modelles inklusive Anbindung an bestehende Systeme

4.8 Leistungspaket H - Konzeption, Realisierung und Betrieb sowie Betriebssupport einer Cloud native Open Source Suite sowie einer passenden Open Source Client Workstation

Der AN hat mit Abschluss eines oder mehrerer leistungskonkretisierender Einzelaufträge unter diesem Rahmenvertrag im Leistungspaket „Konzeption, Realisierung und Betrieb sowie Betriebssupport einer Cloud nativen Open Source Suite sowie einer passenden Open Source Client Workstation“ insbesondere folgende Vertragsleistungen zu erbringen:

- Aufsetzen und Durchführung des Supports für Endanwender
  - Durchführung eines Feldversuchs (Pilot) mit Nutzern vor abschließender Realisierung
  - Zum Feldversuch (Pilot) werden Testkriterien erstellt und zwischen AG und AN abgestimmt, die den AG bzw. die Bw in die Lage versetzen, die Nutzbarkeit der Cloud native Open Source Suite für die Bw zu verifizieren und zu bestätigen.
  - Aufsetzen und Durchführung eines Projektmanagement- und Berichtswesen.
- Die Cloud native Open Source Suite umfasst in einer Konfiguration im Wesentlichen die folgenden Funktionsblöcke:
  - E-Mailkommunikation, Kalender, Kontakte,
  - Dateimanagement (Datenablage, Textverarbeitung, Tabellenkalkulation, Präsentationen),
  - Projektmanagementtool
  - Wissensmanagementtool
  - Zeichentool/ Whiteboardtool
  - Verwaltung für Berechtigungen und Funktionen der Nutzer in der Suite
- Projektierung, Realisierung und Betrieb einer Open Source Client Workstation durch den AN, kompatibel zur Cloud nativen Open Source Suite. Die durch den AN verwendeten Open Source Produkte werden vom AN mit dem AG abgestimmt. Ziffer 9 des Rahmenvertrages bleibt hiervon unberührt.
  - Abstimmung mit DEUmilSAA bezüglich der Akkreditierbarkeit sowie der Akkreditierung der Lösungsansätze zur „Sicheren Architektur für einen SouvAPBw“
  - Abstimmung mit dem BSI bezüglich der Umsetzung der Vorgaben der aktuellen Version des BSI IT-Grundschutz in den Lösungsansätzen zur „Sicheren Architektur für einen SouvAPBw“

- Weiter erfolgt eine
  - Integration des BwMessenger in die Cloud native Open Source Suite
  - Integration der Cloud nativen Open Source Suite in das IAMBw bzw. ITSysBw
  - Integration Funktionsblock Videokonferenz

-
- Die Cloud native Open Source Suite orientiert sich in der Konzeption und Implementierung bei der verwendeten containerisierten Open Source Software am Produkt openDesk des BMI/ ZenDiS bzw. an den Softwareprodukten die im openCode Repository des Bundes bereitgestellt werden.
- Inhaltliche Abstimmung, Beschreibung und Einholung von Freigaben in Bezug auf Lösungs- und Servicekonzepte mit den Betriebseinheiten und Service Architekten des AG
  - Fachliche/inhaltliche Erstellung des Solution Designs und Leistungsbeschreibung
  - Sicherstellen der fachbereichsübergreifenden Konsistenz und Durchgängigkeit der Solution / des Service (End to End)
- Bereitstellen einer vollständigen und aktuellen SBOM zu den verwendeten Softwarekomponenten durch den AN.
- Erstellung eines Migrationskonzepts sowie Planung und Durchführung von Migration bestehender Groupware Collaboration Nutzer der Bw auf die Cloud native Open Source Suite in Abstimmung mit AG.
- Konzeption und Integration bestehender IT-SysBw Systeme in die Cloud native Open Source Suite bzw. der Open Source Workstation in Abstimmung mit AG und Nutzerorganisation.
- Realisierung und Durchführung eines Lifecycle Management, um veränderten und künftigen Anforderungen bzw. neuen Funktionsblöcken gerecht zu werden.
  - Aufsetzen und Betrieb einer produktionsnahen Testumgebung zur Cloud native Open Source Suite
  - Ableitung und Durchführung von Solution Tests bei der Vorbereitung des Solution Deployments und Migration.
  - Weiterentwicklung der Fähigkeiten der Cloud native Open Source Suite bzgl. Anforderungen der Bw (z.B. Offline- / Verlege- Fähigkeiten)
- Projektierung, Realisierung und Durchführung eines Lizenz Management
  - Der AN führt regelmäßig (Zyklus wird in Abstimmung mit AG festgelegt) die notwendigen Prüfungen der Lizenznutzungsbedingungen von OSS Komponenten der Suite (Software Bill of Material) im Sinne der Bw durch und informiert den AG rechtlich belastbar, ob die rechtlichen Anforderungen erfüllt werden und spricht Empfehlungen aus.
  - Das Prüfungsergebnis wird dem AG in nachvollziehbarer Form vor Implementierung (Releaseupdates) der Softwareprodukte bereitgestellt.
- Betrieb der Cloud native Open Source Suite sowie des Open Source Client Workstation in Kooperation und Kollaboration mit den Betriebseinheiten des AG
  - Erstellung Betriebskonzeption und Dokumentation in Abstimmung mit dem AG

- Durchführung initialer und regelmäßiger Trainings des Betriebspersonals des AG
- Erstellung eines Schulungskonzepts für Betriebspersonal des AG
- Etablierung und Durchführung eines Nutzersupports für die Bw Endanwender der Cloud native Open Source Suite basierend auf einem durch den AN zu erstellenden Konzept.

- Schaffung von Service- und Support-Strukturen für die Cloud native Open Source Suite sowie Open Source Client Workstation
  - Aufsetzen und Durchführung eines Incident- Problem- Change Management durch den AN in Abstimmung mit AG und Nutzerorganisation
    - Sicherstellung und Koordination eines direkten hochprioren Last Level Support bei den Softwareherstellern der in der Cloud nativen Open Source Suite verwendeten Produkte.
    - Koordination und Steuerung von Incident- Problem- Change Management durch den AN

4.9 Leistungspaket I - Aufbau Application Stack

Der AN hat mit Abschluss eines oder mehrerer leistungskonkretisierender Einzelaufträge unter diesem Rahmenvertrag im Leistungspaket „Aufbau Application Stack“ insbesondere folgende Vertragsleistungen für die IT-Plattformen zu erbringen:

4.9.1 Aufbau Application Stack in Liegenschaften der Bw

Der Auftragnehmer unterstützt bei Konzeption, Implementierung und Betrieb der Instanzen der IT-Plattform in den Bw-Liegenschaften (BwKrhs Koblenz, Berlin, Ulm und Hamburg und ggf. weiteren Dienststellen des Sanitätsdienstes) und leistet dafür auch entsprechenden 2nd- und 3rd-Level Support, d.h. er erbringt Implementierungs- und Supportleistungen.

4.9.1.1 Leistungen Application Stack

- Unterstützung bei Integration der Hardware der IT-Plattform in den Liegenschaften
  - Planung RZ-Integration (Planung Kühlung, Strom)
  - Aufbau und Implementierung der Hardware-Komponenten in die Betriebsräume der Liegenschaften
- Leistungen zur Regeneration der Hardware der IT-Plattform in den Liegenschaften
- Leistungen zur Netzwerk-Integration der Instanzen der IT-Plattform, Sicherstellung der Kommunikation ins IT-SysBw sowie in die Netze der BwKrhs (nH-Secure) bei Sicherstellung der geforderten Utility sowie Umsetzung der Sicherheitsanforderungen
- Leistungen zur Konzeption und Anbindung eines Identitiy Services der IT-Plattform an das IAM des AG zur nahtlosen Authentifizierung von Nutzern
- Leistungen zur Pflege der Plattform-Software nach Vorgabe des Herstellers. Dies beinhaltet regelmäßige Software, Firmware- und Plattform- Aktualisierungen
- Leistungen zur Bereitstellung der Betriebsmodelle IaaS, PaaS und SaaS in den Liegenschaften des Auftraggebers. Dies umfasst die Unterstützung bei Entwicklung,

Ausrollen und Aufrechterhaltung standardisierter Betriebsabläufe und -verfahren des Auftraggebers.

- Leistungen zur Implementierung und fortlaufender Anpassung technischer und organisatorischer Maßnahmen (TOMs), basierend auf den Anforderungen der BSI und Best Practices im Bereich Datenschutz und IT-Sicherheit
- Leistungen zur Erstellung und Fortschreibung der Informationssicherheitskonzepte und Datenschutzkonzepte, sowie die Unterstützung von Audits (z.B. DEUMilSAA Akkreditierung)
- Leistungen zur Planung und Durchführung Backup/Recovery und Desaster Recovery sowie ggf. Planung und Implementierung einer Replikation in einen alternativen Standort (Geo-Redundanz)
- Leistungen zur Implementierung eines Rollen- und Rechtemodells, dass die Delegation von administrativen Aufgaben an dedizierte Rollenträger beim AG ermöglicht
- Leistungen zur Weiterentwicklungs- und Integrationsleistungen im Rahmen des Life Cycle Managements, Änderung der betrieblichen Umgebung, Integration von Schnittstellen, Einsatz von neuen Technologien und Erzielung von Effizienzsteigerungen.
- Leistungen zur Einrichtung und Nutzung von Application Containern und VM Runtime für virtueller Maschinen sowie Orchestrierung beider Komponenten über Kubernetes
- Leistungen zur Bereitstellung und Weiterentwicklung von Standard Workloads (Secure Windows OS, Linux OS) und Updates der Betriebssysteme nach Vorgaben der Hersteller. Dies beinhaltet Härtungsmaßnahmen am Betriebssystem nach Vorgabe des BSI und der Bw.
- Leistungen zum Betrieb und der Härtung von Middleware (WebServer, OS, Database) nach Vorgabe des BSI und der Bw.
- Leistungen zur Bereitstellung und Management einer virtuellen Desktop Infrastruktur (Citrix VDI) für die Bereitstellung der Anwendungen auf Server- oder Client OS.
- Leistungen zur Entwicklung von Applikations-Schnittstellen sowie bei der Integration ins IT-SysBw
- Leistungen zur Bereitstellung und Konfiguration von File- und Printservices, um eine nahtlose Nutzung und Integration von Peripheriegeräten in die Applikationen zu gewährleisten
- Leistungen zur Migration von Verfahren und Anwendungen auf die IaaS-Plattform insbesondere bei der Migration von VM-ESXI basierenden Workloads in Application Container
- Leistungen zur Erstellung und Weiterentwicklung einer Migration-Roadmap sowie eines entsprechenden Reportings für die Migration von GesVers Anwendungen auf die Zielplattform

4.9.1.2 Supportleistungen

- Leistungen zum 2nd- und 3rd-Level-Support für die IT-Plattformen sowie die betreuten Anwendungen in den Liegenschaften
- Leistungen zur Entwicklung und Implementierung standardisierter Serviceprozesse (ITSM) unter Berücksichtigung der beim Auftraggeber etablierten Strukturen (Incident- Change- und Problemmanagement)

- Leistungen zur Bereitstellung eines Berichtswesens, das regelmäßige Updates über den Fortschritt und die Leistung der erbrachten Vertragsleistungen enthält

4.9.1.3 Application Management

- Leistungen für den Betrieb von Applikationen sowie Durchführung eines Application Managements (Updates, Patches, Herstellerkommunikation, Integration, Support) für Applikationen
- Leistungen zur Erstellung und Bereitstellung von Log- und Eventfiles für die verantworteten Applikationen bzw. Systeme anhand der Vorgaben des Auftraggebers
- Leistungen zur Bereitstellung und Verwaltung von virtuellen Maschinen für Anwendungen und deren Komponenten
- Leistungen zur Bereitstellung und Verwaltung von Anwendungen mit der Kubernetes Engine der IT-Plattform
- Leistungen zur Erstellung und fortlaufender Pflege einer Betriebsdokumentation für Applikationen und deren Systeme (Betriebshandbuch, Konfigurationsdokumentation, Wartungsprotokolle und anderer für den Betrieb notwendigen Dokumente) über die verantworteten Services
- Leistungen zur Durchführung eines proaktiven Monitorings aller verantworteten Komponenten und Software-Produkte
- Leistungen zur Bereitstellung eines Lizenzmanagements für Miet-Software
- Leistungen zur Verwaltung (Asset Management) von Anwendungen sowie Erstellung automatischer Reports für Miet-Software und vom AG beigestellte Lizenzen
- Leistungen zur Durchführung von Schwachstellenanalysen und Empfehlung von Härtungsmaßnahmen an allen Applikationen gemäß den festgelegten Sicherheitsrichtlinien

4.9.1.4 Testmanagement für Anwendungen

- Leistungen zur Bereistellung und Betrieb einer Test- und Integrationsumgebung für Anwendungen
- Leistungen zur Erstellung von Testprotokollen bei Updates und Patches von Anwendungen und deren Komponenten
- Leistungen zur Erstellung von Freigaben mit Fachandwendern und entsprechende rechtssichere Dokumentation

4.9.2 Aufbau Application Stack im Rechenzentrum des AG

Der Auftragnehmer hat Leistungen zur Konfiguration und Betrieb einer mandantenfähigen Verwaltungsstruktur der IT-Plattform für die GesVersBw im zentralen Rechenzentrum des AG auf Erweiterungs-Racks einer vorhandenen Zentralinstanz zu erbringen.

4.9.2.1 Leistungen zentraler Application Stack

- Leistungen zur Durchführung eines PoCs
  - Leistungen zur Erstellung einer Konzeption für die Bereitstellung von GesVers – Anwendungen (über App-Container oder VM-basiert)

- Leistungen zur Konzeption und bei Migration vorhandener Anwendungen (toolbasierte Migration von ESX-VMs in Zielplattform)
- Leistungen zur Bereitstellung von definierten Applikationen, Prüfung und Implementierung der Schnittstellen und bei Integration in Netze der BwKrhs sowie das IT-SysBw
- Leistungen zur Definition und Implementierung der ITSM-Prozesse
- Leistungen zum Support der Applikationskomponenten der Test-Umgebung

- Leistungen zur Überführung der Test-Instanz in einen produktiven Betrieb

5 Beauftragungsmodelle

Die vom AN jeweils zu erbringenden Vertragsleistungen werden vom AG je nach Leistungsgegenstand entweder als Werk- oder Dienstleistung über einen oder mehrere Einzelaufträge unter diesem Rahmenvertrag beauftragt.

Die Leistungserbringung erfolgt in der Regel remote. Etwaige Leistungsorte werden in der jeweiligen Leistungsbeschreibung zum Einzelabruf konkretisiert.

Zudem bestimmen die Parteien im jeweiligen Einzelauftrag – soweit erforderlich, unter Berücksichtigung der Dauer des Onboardingprozesses des AG - in diesem Zusammenhang den jeweiligen Leistungsbeginn der vom AN zu erbringenden Vertragsleistung.

5.1 Dienstleistung

Sofern es sich bei den vom AN zu erbringenden, vom AG beauftragten Vertragsleistungen um Dienstleistungen handelt, erfolgt die Vergütung der Vertragsleistungen durch den AG auf Stundenbasis auf der Grundlage der nachfolgenden Rollenprofile, des Preisblattes/Leistungsverzeichnisses (**Anlage 2** zum Rahmenvertrag) sowie der Regelungen des Rahmenvertrages.

5.1.1 Rollenprofile

Die Parteien stimmen sich vor Abschluss des jeweiligen Einzelauftrages über die für die jeweilige Dienstleistung benötigten Skill-Level und die weiteren Details (u.a. Leistungszeitraum und -ort) sowie die damit verbundene Vergütung auf Grundlage der Regelungen des Preisblattes/Leistungsverzeichnisses ab und schließen einen entsprechenden Einzelauftrag im Sinne der Regelungen des Rahmenvertrages.

Der AN hat im Rahmen der Erbringung der Vertragsleistungen folgende Rollenprofile in jeweils fünf unterschiedlichen Skill-Leveln bereitzustellen:

- **Junior** - 2 Jahre Erfahrung im Themengebiet
- **Regular/Consultant** - 3 Jahre Erfahrung im Themengebiet
- **Senior** - 5 Jahre Erfahrung im Themengebiet
- **Lead** - 6 Jahre Erfahrung im Themengebiet
- **Executive** - mehr als 6 Jahre Erfahrung im Themengebiet

Rollenprofil	Beschreibung	Aufgaben/Fähigkeiten
Agile Master	Der Agile Master trägt die Verantwortung für die Umsetzung und Einhaltung agiler Prinzipien, Frameworks und Arbeitsweisen. Er begleitet ein oder mehrere Teams im Rahmen der Leistungserbringung als Methodenexperte. Der Agile Master identifiziert Möglichkeiten zur Produktivitätssteigerung des/der Agile Teams im Sinne eines Servant Leaders. Er schützt dabei das Agile Team vor äußeren Einflüssen, sichert den agilen Prozess und beseitigt Hindernisse, die den Fortschritt des/der Agile Teams behindern.	• trägt die formale Verantwortung für agile Prinzipien, Frameworks und Arbeitsweisen • fördert proaktiv das gegenseitige Vertrauen in die Prozesse des agilen Teilprojekts • macht zusammen mit dem/der Product Owner die Prozesse des agilen Teilprojekts gegenüber den Stakeholdern transparent
Cloud Developer	Der Cloud Developer bewertet und unterstützt die Geschäftsziele Produkte und Dienste aus Sicht der Cloud-Anwendungen. Er automatisiert Workloads und Prozesse. Er definiert in enger Zusammenarbeit mit anderen Experten Software-Architektur mit Microservices. Er kümmert sich um kontinuierliche Integrations- und Deploymentprozesse und stellt die effiziente Zusammenarbeit in (Sec)DevOps Teams sicher.	• Beherrschung von Cloud-Mechanismen, -Werkzeugen und Kenntnisse von Anbietertechnologien (GDC, VCF, Container, Kubernetes usw.) • Kontinuierliche Integration und DevOps • Professionelle Software-Entwicklung • Anwendung agiler Projektmanagement-Methoden • Automatisierung und Optimierung von Linux Systemen mit Command-line Schnittstellen zur (z.B. gdcloud CLI) • Erfahrung mit Infrastructure as Code • Betrieb von Open Source-basierten Virtualisierungs- und Containerumgebungen (z.B. mit Kubernetes oder KubeVirt) • Erfahrung mit Cloud-nativen Technologien (z.B. SAP BTP, GIT, Spring und Docker) • Vertrautheit mit Clean Code, Peer Review und Pair Programming

IT-Architect	Der IT-Architect entwirft und plant die IT-Infrastruktur eines Unternehmens, um sicherzustellen, dass sie skalierbar, sicher und effizient ist. Er arbeitet mit verschiedenen Teams zusammen, um IT-Lösungen zu entwickeln, die den Geschäftsanforderungen entsprechen. Zu den Aufgaben gehören die Analysen bestehender Systeme, das Design neuer Architekturen, die Auswahl von Technologien sowie die Erstellung technischer Dokumentationen. Der IT-Architect stellt sicher, dass alle IT-Systeme integriert, funktional und zukunftssicher sind.	• Zusammenarbeit mit Führungskräften, um Lösungen mit den Geschäftszielen in Einklang zu bringen • Durchführung von Analysen zur Identifizierung von Schwachstellen und Anforderungen für Verbesserungsinitiativen • Entwicklung umfassender Architektur- und Integrationspläne für komplexe Technologieprojekte • Koordination von Ressourcen und Anbietern über funktionsübergreifende Teams hinweg, um die Projektumsetzung sicherzustellen • Überwachung der Phasen von Design, Entwicklung, Tests, Schulungen und Implementierung von Lösungen • Überwachung von Projekten auf höchster Ebene • Management von Risiken, Problemen und Umfangserweiterungen über den gesamten Lebenszyklus der Initiative hinweg • Sicherstellung der Einhaltung von Richtlinien, Standards und behördlichen Vorschriften
Modellierer	Ein Modellierer ist verantwortlich für die Erstellung und Pflege von Modellen, die komplexe Systeme, Prozesse und Strukturen visualisieren und verständlich machen. Mithilfe von Modellierungsstandards (NAF, BPMN) übersetzt er Anforderungen in präzise Darstellungen, die als Grundlage für die Systementwicklung, Optimierung oder Analyse dienen. Der Modellierer arbeitet eng mit Fachabteilungen zusammen, um sicherzustellen, dass die Modelle den tatsächlichen Anforderungen entsprechen und unterstützt die kontinuierliche Verbesserung von Prozessen. Dabei dokumentiert er alle Modelle und stellt sicher, dass sie korrekt und aktuell sind.	• Modellierung von System-Umgebungen innerhalb von Sparx Enterprise Architect unter Verwendung einer Modellierungssprache, die eine Teilmenge des ADMBw darstellt. Die Modellierung setzt voraus, dass sehr ausgeprägte IT-Kenntnissen vorhanden sind. • Teilnahme an Workshops zur Festlegung der System-Komponenten. • Verwaltung und Zuordnung von Automatisierungs-Software-Code zu den System Elementen. • Scripting in Sparx Enterprise Architect zur Modellpflege. • Dokumentation der Systeme aus Sparx Enterprise Architekt heraus. • Unterstützung bei der Testung der automatisierten System-Umgebungen. • Modellierung von Architekturen in ADMBw.

Product Manager	Die Rolle des Product Managers ist verantwortlich für die Übersetzung der Vision und des Zielbildes in operative Themen. Sie trägt somit die inhaltliche Gesamtverantwortung teamübergreifend für das Gesamtprodukt. Der Product Manager unterstützt und stellt eine zielgerechte technische Umsetzung der Produktteams sicher. Er berücksichtig dafür den Input der relevanten internen & externen Stakeholder und stimmt sich hierbei eng mit der Gesamtprojektleitung ab.	• Entwicklung und Pflege der Produtkstrategie und –vision. • Erstellung und Verwaltung der Produkt-Roadmap. • Durchführung von Markt- und Wettbewerbsanalysen. • Sammlung und Analyse von Markt- und Wettbewerbsanalysen. • Sammlung und Analyse von Kundenfeedback und Marktdaten. • Definition und Priorisierung von Produktanforderungen. • Zusammenarbeit mit funktionsübergreifenden Teams. • Steuerung der Produktentwicklung und Sicherstellung der termingerechten Umsetzung.
Product Owner	Product Owner bezeichnet die Rolle mit dem größten Wissen über das zu kreierende Produkt. Der Product Owner steuert durch die Priorisierung der Einträge im Product-Backlog nach Business Value die Aufgaben des Teams und ist Ansprechpartner für eine kontinuierliche Produktentwicklung. Das setzt voraus, dass der/die Product Owner ständig in den Informationsfluss mit dem Kunden eingebunden ist und sich eng mit der Gesamtprojektleitung abstimmt.	• Definition und Priorisierung des Product Backlogs • Sicherstellung, dass das Entwicklungsteam die Produktanforderung versteht • Enge Zusammenarbeit mit Stakeholdern, um Anforderungen zu sammeln und zu verfeinern • Formulierung von klaren User Stories und Akzeptanzkriterien • Teilnahme an Scrum Events wie Sprint Planning, Daily Standups und Sprint Reviews • Entscheidung über Prioritäten und Anpassungen im Sprint • Verantwortung für die Produktvision und deren Kommunikation im Team • Abnahme von fertigen Inkrementen und Sicherstellung der Qualität • Sicherstellung, dass das Produkt den geschäftlichen Anforderungen entspricht und Mehrwert liefert

Project Management Office	Das PMO definiert die Standards für das Projektmanagement innerhalb der Organisation und erhält sie aufrecht. Das PMO strebt eine Standardisierung und Optimierung bei der Durchführung von Projekten an. Das PMO ist die Quelle für Dokumentationen, Anleitungen und Kennzahlen zur Praxis des Projektmanagements und der Projektausführung. Es kann auch als interner Dienstleister für einzelne Projekte fungieren, indem es bei ausgewählten Projektmanagement-Aufgaben unterstützt.	• behält den Überblick über das Projektportfolio • bereitet Entscheidungsgrundlagen vor und erleichtert die Entscheidungsfindung für das Portfolio-Board • plant Ressourcen auf Portfolioebene und optimiert den Ressourceneinsatz • standardisiert die Methoden und Prozesse im Projektmanagement • wählt geeignete PMO-Tools oder Software-Lösungen aus und führt sie ein, einschließlich der Schulung der Mitarbeiter • schafft Transparenz über aktuelle und geplante Projekte durch Bereitstellung aktueller, zuverlässiger Projektdaten • fördert den Informationsfluss und die Kommunikation • überwacht die Projektfortschritte und steuert die Abhängigkeiten, die sich auf Ressourcen, Budgets und Zeitpläne auswirken • bietet administrative und operative Unterstützung für Projektleiter und Projektteams, z.B. im Bereich des Konfliktmanagements, der Workshop-Moderation und des Controllings

Projekt Manager	Der Projekt Manager übt seine Aufgaben dauerhaft aus und steht dem Bereich als Projektmanagement-Fachmann für verschiedene Projektmanagement-bezogene Themen zur Verfügung. Meistens wird er die temporäre Rolle des Projektleiters übernehmen. Allerdings ist die Projektleitung oder Mitwirkung an Projekten nicht auf Mitarbeiter des Business Managements beschränkt. Der Projektleiter trägt die Gesamtverantwortung für ein Projekt in allen Phasen, d.h. er muss das Projekt konzipieren, planen und initiieren, durchführen und auch abschließen. Ziel ist es, eine beauftragte Lösung vertragskonform im Rahmen von definierten Scope-, Zeit-, Kosten- und Qualitätsvorgaben zu liefern. Der Projektleiter wird vom Projektsponsor/Entrepreneur ernannt. Er sorgt dafür, dass die definierten Ergebnisse zeitgerecht, im Kostenrahmen und in der gewünschten Qualität erreicht werden.	• Projektleitervereinbarung mit Internem Auftragnehmer abstimmen • Projektumfang und -organisation definieren, strukturieren, detaillieren, planen (Scope, Time, Quality) und Freigabe des Internen Auftragnehmers einholen • Abhängigkeiten zu anderen Projekten/Programmen/Organisationseinheiten (intern/extern) identifizieren und beschreiben • Zusammenarbeit mit PM-Paten aktiv gestalten; von der Vorhaben-Klassifikation bis hin zu Projektabschluss vorbereiten • Projektplan erstellen und managen • PQG-Unterlagen erstellen und Freigabe vom Internen Auftragnehmer für die nächste Projektphase einholen • Die Stakeholder (intern/extern) identifizieren und in die Kommunikation einbinden • Mitwirkungshandlungen und Beistellungen mit Kunde/AG vereinbaren • Projektablage in DMS einrichten und pflegen • Ressourcen planen und anfordern, Projektteam organisieren und managen (Engpässe eskalieren) • Lieferanten und Unterauftragnehmer managen • Risikomanagement im Projekt sicherstellen • Offene Punkte identifizieren und managen • Projektänderungen bewerten und bei Genehmigung umsetzen • Berichterstattung, Vorbereitung von Entscheidungen, Präsentieren des Projekts und Projektmarketing durchführen • Projektdokumentation sicherstellen • Monatl. Projektstatusbericht erstellen (Projektstatus inkl. Risiken und Finanzstatus) • Zahlungsbegründende Unterlagen dokumentieren, Abnahmen planen, vereinbaren, einholen, dokumentieren • Vorbereitung und Teilnahme an Projektstatusupdates • Teilnahme an vorhabeninternen Gremien des Projekts

		• Umsetzung von PPM Maßnahmen nach Entscheidung durch das PPM Board (z. B. Anpassung der Planung nach erfolgter Umwidmung) • Projektabschlussbericht erstellen • Lessons Learned durchführen • Lessons Learned Ergebnisse besprechen, dokumentieren und zur Veröffentlichung in die Lessons Learned Wissensdatenbank der DBI senden
Business Architect	Der Business Architect unterstützt und gestaltet bei der Einführung, Umsetzung und Automatisierung von Prozessen im Kontext IT-Management. Er nimmt Anforderungen auf, analysiert Prozesse bzw. vorhandene Digitalisierungslösungen und unterstützt bei der Umsetzung innovativer neuer Lösungen. Darüber hinaus modelliert er Prozess und stimmt diese mit den Stakeholdern ab.	• Use Case- sowie Anforderungserhebung und –formulierung • Analyse von Prozessen und IT-U-Lösungen sowie Ableitung von Optimierungspotentialen • Unterstützung zu Fragestellungen interner und externer Kunden zum Thema Prozesse • Konzeption von Lösungen in Zusammenarbeit mit IT-Architekten aus unterschiedlichen Fachbereichen • Modellierung von Prozessen mit gängigen Tools (z.B. Aris) und Frameworks (z.B. BPMN)

Solution Architect	Der Solution Architekt plant, steuert, überwacht und koordiniert die fachlich/inhaltliche Solution Entwicklung bis zur Abnahme durch den Auftraggeber, mit dem Ziel eines effizienten Designs der geplanten Kundenlösung. Er unterstützt dabei den AG bei der ganzheitlichen Betrachtung der Kundenlösung. Dabei stimmt er sich eng mit den relevanten Stakeholdern ab.	• Erstellung des Solution Designs und Dokumentation in der Solution Beschreibung • Zuarbeit bei Erstellung und Fortschreibung von IT-Sicherheitskonzepten • Durchführung von Solution Designs nach EPDF • Unterstützung und Beratung bei der Konzeption der Test- und Integrationsphase der Solution (Solution Test) • Unterstützung und Beratung bei der Einführung der Solution (Solution Transition), d.h. bei Konzeption von Daten- / User-Migrationen, Konzeption von Proof of Concepts und Pilotphase (Early Life Support) • Teilnahme an Quality Gates • Zentrale Ablage / Archivierung des an den Solution Delivery Manager übergebenen Dokumentationsstandes zum Solution Release • Erstellung weiterer Projekt- oder Kunden-spezifischer Dokumente nach Absprache
System Engineer	Der System Engineer ist ein Fachexperte, der komplexe technische Systeme entwickelt und verwaltet. Er stellt sicher, dass IT-Systeme effizient funktionieren, robust sind und den Anforderungen der Nutzer entsprechen. Er ist verantwortlich für die Integration von Hardware und Software, das Testen, die Fehlerbehebung und die Optimierung der Systemleistung. Er stellt sicher, dass die Systeme reibungslos und zuverlässig arbeiten und den spezifischen Bedürfnissen der gehosteten Applikationen gerecht werden.	• Implementierung und Anpassung neuer sowie bestehender Systeme • Überwachung und Bewertung der Geschäftsauswirkungen • Analyse der System-Effizienz, Fortlauffende Optimierung der Systeme • Identifizierung von Verbesserungspotenzialen • Erstellung von Berichten und Präsentationen • Automatisierung der Systeme (u.a. über Scriptsprachen) • Sicherstellung der Datensicherheit der Systeme, einschließlich der Einhaltung von Compliance-Anforderungen und der Durchführung von Sicherheitsprüfungen.

Military Industry Consultant	Ableitung, Definition und Validierung zur Umsetzung von cloudbasierten Technologien in Fü(W)ES der Bw, zum Fähigkeitserhalt und der Fähigkeitserweiterung.	• Vertiefende Kenntnisse in der Integration bestehender und zukünftiger FüWaEinsSys • Modellierung von Prozessen mit gängigen Tools (z.B. EA Sparx) und Frameworks (z.B. NAFv4/ ADMBw) • Implementierung und Anpassung neuer und bestehender FüWaEinsSys sowie der Analyse der System-Effizienz, einer fortlaufenden Optimierung der Systeme • Technologien in bestehende FüWaEinsSys integrieren, adaptieren und verproben • Identifikation, Anpassung und Weiterentwicklung von Use Case- sowie Anforderungserhebung und –formulierung im Zuge der Implementierung und Adaption in und von FüWaEinsSys • Validierung und Verifizierung, von FüWaEinsSys in Hinblick auf Interaktion und Anpassbarkeit neuer Technologien • Identifizierung und Validierung von Verbesserungspotenzialen zum Einsatz neuer Technologien in FüWaEinsSys • Erstellung von Berichten und Präsentationen • Herstellung von IT-Sicherheit und Datensicherheit sowie Betriebssicherheit von FüWaEinsSys

5.1.2 Rufbereitschaft

Auf Veranlassung des AG erbringt der AN im Rahmen seiner Leistungserbringung eine Rufbereitschaft zu den nachfolgend beschriebenen Rahmenbedingungen, sofern dies nach den jeweils gültigen Betriebsvereinbarungen des AN zulässig ist. Der genaue Umfang und die konkret vom AN zu erbringenden Vertragsleistungen werden im jeweiligen Einzelauftrag konkretisiert.

Bei Einzelaufträgen mit Rufbereitschaft wird im jeweiligen Einzelauftrag sowohl die Menge der beauftragten Stunden je Rollenprofil („Basismenge“) sowie zusätzlich die beauftragte Menge der hierbei jeweils zu leistenden Stunden an Rufbereitschaft hinterlegt. Dabei kann die Menge der Stunden für Rufbereitschaft maximal 50% der Basismenge betragen. Sobald die Basismenge ausgeschöpft ist, kann ein ggf. noch vorhandenes Kontingent aus Rufbereitschaft nicht mehr abgerufen werden. In diesem Fall stimmen die Parteien einen neuen Einzelauftrag

ab. Grundlage zur Bestimmung der bereits geleisteten Basismenge ist die Faktura.

Bevor Ressourcen des AN erstmalig im Rahmen einer Rufbereitschaft für den AG aktiv unterstützen können, benötigt der AN einen Vorlauf von bis zu 3 Monaten um den Voraussetzungen aus Arbeitsrecht und Betriebsvereinbarungen zu entsprechen. Diesen Prozess kann der AN bereits vor der tatsächlichen Beauftragung des Einzelauftrags starten, sofern vom AG die dafür notwendigen Informationen rechtzeitig vorab bereitgestellt werden. Die Leistungserbringung des Einzelauftrags an Tätigkeiten außerhalb der Rufbereitschaft ist von dieser Frist unberührt und beginnt mit dem im Einzelauftrag vereinbarten Liefer- und/oder Leistungstermin.

Das im Einzelauftrag beauftragte Verhältnis aus Rufbereitschaft zu Basismenge darf bei der späteren Abnahme von Rufbereitschaft und Basismenge nicht überschritten werden.

a) Zeitraum und Dauer der Rufbereitschaft
Der AN stellt auf Veranlassung des AG während des vereinbarten Zeitraums (an Arbeitstagen zwischen 17:00 – 07:00 Uhr, an Wochenenden 0:00 – 24:00 Uhr, an bundeseinheitliche Feiertagen 0:00 – 24:00 Uhr) eine Rufbereitschaft zur Verfügung.

b) Reaktionszeit der Rufbereitschaft
Der AN verpflichtet sich, während der vereinbarten Rufbereitschaft jederzeit unter der vereinbarten Telefonnummer erreichbar zu sein, um auf Anfragen des AG innerhalb von 60 Minuten zu reagieren, d. h. der AN ist innerhalb dieses Zeitraums technisch in der Lage, Ursachenforschung in den betroffenen Systemen zu betreiben bzw. mit der Fehlerbehebung zu beginnen, wobei sich die vorgenannten Tätigkeiten des AN auf die Vertragsleistungen des jeweiligen Einzelauftrags beziehen.

c) Tätigkeiten der Rufbereitschaft
Die Rufbereitschaft umfasst die Beantwortung und Bearbeitung von dringenden Anfragen des AG innerhalb der unter a) vereinbarten Rufbereitschaftszeit. Die genauen Arten von Anfragen sowie die vom AN jeweils in diesem Zusammenhang zu erbringenden Tätigkeiten werden in dem jeweiligen Einzelauftrag konkretisiert.

d) Vergütung der Rufbereitschaft
Die Rufbereitschaft wird auf Basis der vereinbarten Stundensätze auf der Grundlage des Preisblatts/Leistungsverzeichnisses (Anlage 2 des Rahmenvertrages) vergütet.

e) Vergütung für Einsätze während der Rufbereitschaft
Soweit im Rahmen der Rufbereitschaft eine Tätigkeit zur Fehlerbehebung / -entstörung erforderlich ist, wird die vom AN dahingehend erbrachte Vertragsleistung vom AG auf der Grundlage des Preisblatts/Leistungsverzeichnisses (Anlage 2 des Rahmenvertrages) in Verbindung mit den unter Ziffer 11.4 des Rahmenvertrages vereinbarten Zuschlägen vergütet.

5.2 Werkleistung

Sofern der AG die vom AN zu erbringenden Vertragsleistungen über einen oder mehrere Einzelaufträge unter diesem Rahmenvertrag als Werkleistungen beauftragt, gelten die nachfolgenden Regelungen.

5.2.1 Leistungspaket

Die vom Auftragnehmer zu erbringenden Vertragsleistungen sind konkreten Leistungspaketen zugeordnet, für die ein oder mehrere leistungskonkretisierende Einzelaufträge abgeschlossen werden, wobei der bzw. die leistungskonkretisierenden Einzelaufträge unter diesem Rahmenvertrag immer exakt einem Leistungspaket zugeordnet sind.

5.2.1 Sizing

Die Höhe der jeweiligen Vergütung auf Basis eines Festpreises für eine vom AN unter diesem Rahmenvertrag zu erbringenden Werkleistung ist abhängig von dem jeweiligen Aufwand, der Realisierungsdauer und des jeweiligen Komplexitätsfaktors. Die Analyse des jeweiligen Aufwands, der jeweiligen Realisierungsdauer und des jeweiligen Komplexitätsfaktors ermöglichen eine Zuordnung der vom AN zu erbringenden Werkleistungen in eine bestimmte Sizing-Größe (nachfolgend „T-Shirt Größe“ genannt). Jede T-Shirt Größe hat einen auf Basis des Preisblattes/Leistungsverzeichnisses (**Anlage 2** zum Rahmenvertrag) vorgegebenen Festpreis, zu dem das jeweilige Werk beauftragt wird.

Die nachfolgenden Übersichten sollen exemplarisch den Zusammenhang der vorgenannten Messfaktoren zur Eingruppierung in T-Shirt Größen sowie die Ermittlung des Komplexitätsfaktors darstellen. Die Parteien stimmen sich im Rahmen des Abschlusses des jeweiligen Einzelauftrages über die jeweilige Eingruppierung einer Werkleistung in eine T-Shirt Größe ab (vgl. hierzu Ziffer 5.2.2 dieser Leistungsbeschreibung).

Die Richtwerte in der folgenden Tabelle stellen lediglich Orientierungsgrößen dar.

T-Shirt-Größe	Richtwert Aufwand	Max. Realisierungsdauer	Skill Level	Komplexitätsfaktor		
				low	medium	high
XS	80 Stunden	2 Wochen	Consultant	50%	20%	10%
			Senior	30%	50%	30%
			Lead	20%	30%	50%
			Executive	0%	0%	10%
S	160 Stunden	2 Wochen	Consultant	50%	20%	10%
			Senior	30%	50%	30%
			Lead	20%	30%	50%
			Executive	0%	0%	10%
M	240 Stunden	2 Wochen	Consultant	50%	20%	10%
			Senior	30%	50%	30%
			Lead	20%	30%	50%
			Executive	0%	0%	10%
L	360 Stunden	3 Wochen	Consultant	50%	20%	10%
			Senior	30%	50%	30%
			Lead	20%	30%	50%
			Executive	0%	0%	10%
XL	960 Stunden	12 Wochen*	Consultant	40%	20%	10%
			Senior	30%	40%	30%
			Lead	25%	30%	40%
			Executive	5%	10%	15%
XXL	1.920 Stunden	12 Wochen*	Consultant	40%	15%	10%
			Senior	30%	40%	30%
			Lead	20%	30%	40%
			Executive	10%	15%	20%

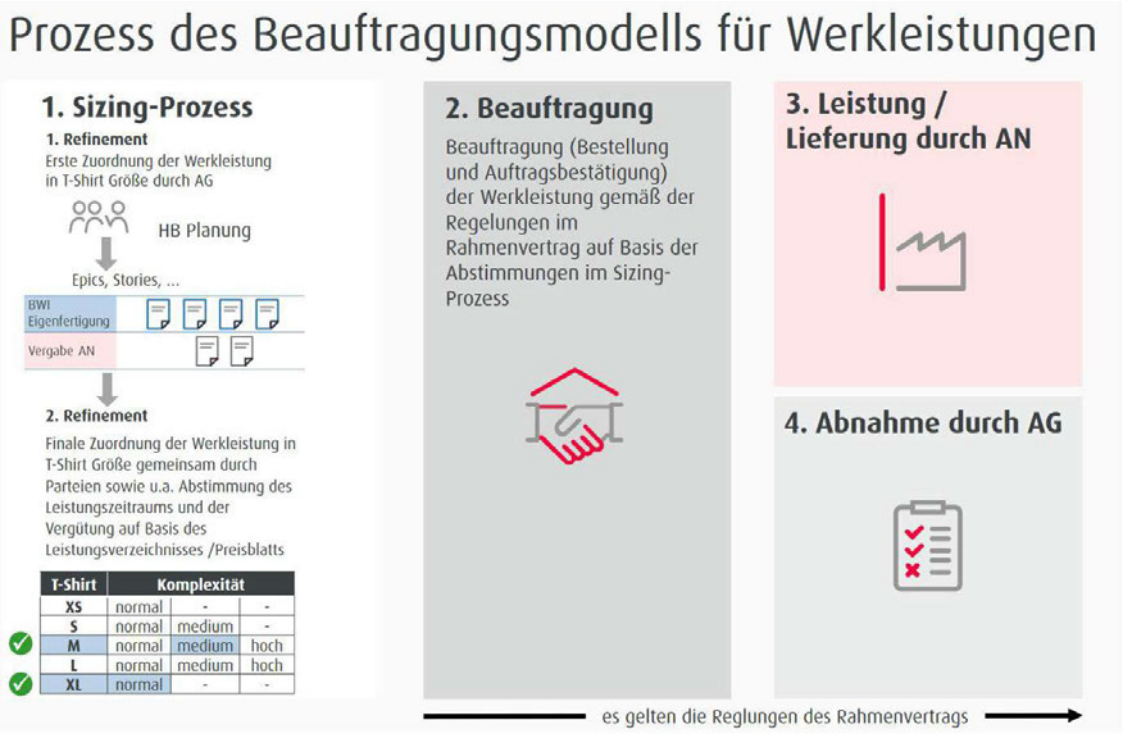
*Die Realisierungsdauer kann im Refinement zwischen den Parteien abweichend vereinbart werden.

Kriterium	Leitfragen	Komplexitätsfaktor		
		low	medium	High
Aufgabenklarheit	• Wie detailliert ist die Aufgabenbeschreibung? • Existiert bereits ein Breakdown von Aufgaben? Wenn ja, wie detailliert?	Hoch	Mittel	Niedrig
Technologie	• Wie gut sind die verwendeten Technologien dokumentiert und etabliert? • Handelt es sich um neue oder experimentelle Technologien?	Etabliert	Teils neu	Innovativ
Ressourcenbedarf	• Wie viel spezialisiertes Fachwissen wird benötigt? • Ist externe Unterstützung erforderlich?	Gering	Mittel	Hoch
Skill-Level	• Welche Skill-Level werden vornehmlich mit der Umsetzung betraut sein? • Welchen Skill-Mix benötige ich für die Umsetzung der Aufgabe?	Junior	Junior, Senior	Senior, Executive
Risiko	• Gibt es viele unbekannte Faktoren oder Unsicherheiten? • Sind erwartbar Risiken mit der Umsetzung der Aufgabe verbunden? • Gibt es bereits Pläne zur Risikominderung?	Gering	Mittel	Hoch
Abhängigkeiten	• Existieren Abhängigkeiten zu Aufgaben oder Systemen? • Gibt es externe Faktoren (außerhalb des direkten Einflussbereichs), die berücksichtigt werden müssen?	Wenige	Einige	Viele

5.2.2 Sizing-Prozess

Der AG nimmt in der Planungsphase zur Beauftragung des AN mit einer Werkleistung über einen Einzelauftrag im Rahmen eines ersten Refinements eine erste Zuordnung der vom AN jeweils zu erbringenden Werkleistung in eine T-Shirt-Größe vor. Dies stellt die Planmenge zur Bestimmung der notwendigen Größe (T-Shirt Größe und Komplexität bzw. Richtwert Aufwand) des daraus resultierenden jeweiligen Einzelauftrags dar.

Vor Abschluss eines entsprechenden Einzelauftrags unter diesem Rahmenvertrag stimmen sich die Parteien im Rahmen eines zweiten Refinements schließlich über die finale Zuordnung in eine T-Shirt-Größe und den Komplexitätsgrad sowie die damit verbundene Vergütung auf Grundlage der Regelungen des Preisblattes/Leistungsverzeichnisses (Anlage 2 des Rahmenvertrages) ab, schließen einen entsprechenden Einzelauftrag im Sinne der Regelungen des Rahmenvertrages und dokumentieren diese Entscheidung. Die nachstehende Abbildung veranschaulicht den Zusammenhang:



6 Beistellleistungen und Mitwirkungsobliegenheiten des AG

Der AG stellt dem AN die nachstehend aufgeführten Betriebsmittel ausschließlich zur Erfüllung des Vertragszweckes zur Verfügung, soweit und solange diese zur Erbringung der Vertragsleistungen durch den AN erforderlich sind und sich aus dem jeweiligen Einzelauftrag nichts Abweichendes ergibt:

- AG – Client (eine technische Anbindung an die Netzinfrastruktur des AG ist ausschließlich über einen sogenannten AG-Client möglich)
- Beistellung und Zugriff auf relevante Software-Applikationen/ Datenbanken
- Zugriff auf die internen Datenmanagementsystem-Ablagen des AG

Die Betriebsmittel sind unter Beachtung der Regelungen aus dem Rahmenvertrag bzw. Einzelauftrag, insbesondere unter Beachtung der Regelungen zur IT-Sicherheit, zum Daten- und zum Geheimschutz zu verwenden. Der AG ist berechtigt, nach eigenem Ermessen und jederzeit innerhalb der Laufzeit des Rahmenvertrages bzw. Einzelauftrags beigestellte Betriebsmittel zurück zu verlangen. In einem solchen Fall wird der AG die zurückgeforderten Betriebsmittel durch adäquate Betriebsmittel ersetzen, sofern und solange dies für die Erbringung der Vertragsleistungen durch den AN erforderlich ist.

Darüber hinaus obliegt dem AG die Erbringung der folgenden Mitwirkungshandlungen, soweit und solange diese für die Erbringung der Vertragsleistungen durch den AN erforderlich ist und sich aus dem jeweiligen Einzelauftrag nichts Abweichendes ergibt:

- Zutritt zu Standorten des Auftraggebers bzw. Endkunden
- Zurverfügungstellung aller benötigten Informationen zum Leistungsgegenstand, bestehend beispielsweise aus:
  - Informationen zu abhängigen Projekten
  - Einblick in relevante Prozesse
- Nennung Ansprechpartner zu den jeweiligen Themengebieten
- Datenlieferungen und sämtliche für die Störungsanalyse und Beseitigung relevanten Informationen (Logfiles, Dumps u.a.)
- Berechtigungen, Zugriffsrechte

7 Anhänge

Anhang	Verbindliche Anforderungen aus der Projektmanagement- Systematik der BWI GmbH

Signatures

Number of pages (including this one): 38

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

Anhang zur Anlage 1 (Leistungsbeschreibung)

- Verbindliche Anforderungen aus der Projektmanagement- Systematik der BWI GmbH -

Inhalt

Inhalt 2

Allgemeines 3

1 PM@BWI – verpflichtend anzuwendende Projektmanagementmethode in der BWI 4

1.1 Rollen 4

1.2 Meetings 5

1.3 Kommunikation 7

1.4 Tooling & Aufgabenmanagement 8

1.5 Dokumentation und Abnahmen 10

1.6 Eskalationswege 11

Verzeichnisse 15

Tabellen 15

Abkürzungen 16

Dokumentenhistorie, Änderungen, Archivierung 16

Allgemeines

Der Auftragnehmer (AN) ist verantwortlich dafür, die Inhalte an seine ausgewählten, eingesetzten eigenen Mitarbeiter vor Einsatzbeginn zu vermitteln, die Beachtung eigenständig zu kontrollieren und eventuelle Abweichungen im Rahmen seines arbeitsorganisatorischen Weisungsrechts sowie seiner Organisations-/Unternehmerentscheidungen zu beseitigen.

Im Falle einer BWI angezeigten und genehmigten Unterbeauftragung ist die Fremdfirma (Auftragnehmer) verpflichtet, ihre entsprechende Pflicht an den Unterauftragnehmer vertraglich weiterzugeben.

1 PM@BWI – verpflichtend anzuwendende Projektmanagementmethode in der BWI

Die unternehmensinterne Projektmanagementmethode der BWI heißt PM@BWI[1] und setzt die Rahmenbedingungen für Projekte. Sie hat das Ziel, eine einheitliche, vertragskonforme und effiziente Abwicklung über die gesamte Kette der Leistungserbringung/ -erbringer zu gewährleisten.

PM@BWI ist eine eigens auf die Bedürfnisse der BWI abgestimmte - in Anlehnung an DIN ISO 21500 "Leitfaden zum Projektmanagement", ISO 10006 "Qualitätsmanagementsysteme; Leitfaden für Qualitätsmanagement" und DIN 69901 "Projektmanagement; Projektmanagementsysteme" - zertifizierte Vorgehensweise.

Das für die Projekte übergeordnete und verpflichtende Rahmenwerk PM@BWI ermöglicht in der operativen Umsetzung der Projekte (Projektdurchführung) sowohl (rein) klassische als auch (rein) agile Methoden und Praktiken. Über deren Effektivität und Effizienz sowie Einsatz entscheidet der Projektverantwortliche (Projektleiter) der BWI im projektspezifischen Kontext. Der Projektverantwortliche sorgt dabei für eine funktionierende, den jeweiligen Umständen entsprechende Projektorganisation (inkl. externer Teilleistungen), führt und unterstützt die Projektbeteiligten sach-/ergebnisbezogen und koordiniert die Abhängigkeiten zwischen den Leistungen.

1.1 Rollen

PM@BWI regelt die in Projekten verbindlich zu besetzenden Rollen, deren wesentliche Aufgaben, Kompetenzen und Verantwortlichkeiten.

Der AN übernimmt innerhalb der PM@BWI die an ihn zugewiesenen Teilleistungen selbständig, in eigener unternehmerischer Organisation und mit eigenen Ressourcen. Er ist kein Teil der Projektorganisation und für die eigenverantwortliche Umsetzung der definierten Leistungspakete, deren Richtigkeit und die rechtzeitige Meldung von Problemen und möglichen Risiken verantwortlich.

[1] Unternehmensinterne Projekt- und Programmmanagementmethode der BWI

Innerhalb der Umsetzung von Projekten in einem Scrum Setup[2] können AN in den Rollen Scrum Master (im Rollenkatalog der BWI Agile Master benannt) oder selbständiger Entwickler eingesetzt werden. Die konkrete Rollenverteilung/Leistung ist im Rahmen des jeweiligen Dienstleistungs- oder Werkvertrag geregelt.

1.2 Meetings

Meetings werden virtuell und in Ausnahmefällen vor Ort abgehalten (s. Kapitel 1.3 Kommunikation). Der AN wird nur dann zu Präsenz-Meetings in BWI-Räumlichkeiten und anderen physischen Meeting-Örtlichkeiten einbestellt, wenn dies zur Vertragserfüllung zweckdienlicher oder erforderlich sein sollte und vertraglich vorgesehen/vorbehalten ist. In diesem Fall bietet der AG im Vorfeld mehrere Möglichkeiten für den AN an und einigt sich mit ihm auf Zeit und Ort der Präsenz-Vor Ort Termine. Die Einigung erfolgt zwischen den im Vertrag definierten Ansprechpartnern von AG und AN.

In einem Scrum Setup beträgt die Sprintlänge mindestens 2 Wochen und beinhaltet dabei diverse Scrum Meetings. Daraus resultiert eine verpflichtende Teilnahme des AN an den Scrum-Meetings, grundsätzlich online via Webex.

Folgende Meetings finden innerhalb eines Scrum Setups statt, deren konkrete Dauer in der jeweiligen Leistungsbeschreibung festgelegt wird:

Termin	Inhalt des Termins
Daily	Kurzes (max. 15 Min.), tägliches Meeting zur Darstellung des IST- Zustandes.
Sprint Planning	Zur Planung und Festlegung der Aufgabenerledigung, welche im nächsten Sprint umgesetzt werden soll.
Sprint Review	Für die Präsentation der Aufgabenerledigung.
Retrospektive	Bietet den Beteiligten die Möglichkeit sich selbst zu überprüfen. Findet zwischen dem Sprint Review und der Sprint Planung statt.
Backlog Refinement	Für den Optimierungsprozess eines Sprint Backlogs.

Tabelle 1: Meetingarten

[2] basiert auf Grundlage des aktuellen Scrum Guide s. https://scrumguides.org/scrum-guide.html

Sofern die Rolle/Leistung des Scrum Masters mit dem AN vertraglich vereinbart ist, übernimmt er die fachliche Planung der Meetings im Auftrag des AG ohne über ein personenbezogenes Weisungsrecht gegenüber den Teilnehmern zu verfügen. Alle Termine, Meetings und die dazugehörige Korrespondenz sollten dokumentiert und Ad-hoc-Meetings vermieden werden.

Für die Definition/Planung der jeweils nächsten vertragsgemäßen Leistungen und Arbeitsergebnisse sowie Abnahmekriterien, des jeweiligen erreichten Umsetzungsstatus und die Vereinbarung kommender Termine findet ein gemeinsames Planungsmeeting statt. Dieses Planungsmeeting soll nach vertraglichen Vereinbarung AG – AN regelmäßig stattfinden und wird in der Leistungsbeschreibung festgelegt.

Online/virtuell via Webex

Präsenz vor Ort in (angemieteten) Räumen des AG findet nur statt, wenn dieses aus ergebnisorientierten Gründen notwendig ist.

Bei Erforderlichkeit können die Parteien ergänzende Planungsmeetings verabreden oder von den vorstehenden Regelungen im Einzelfall abweichen. Die Einigung erfolgt zwischen den definierten Ansprechpartnern von AG und AN.

Der AG (Product Owner) legt im Meeting seine gewünschte Planung/Zielvorstellung der nächsten Iterationen dar und in Abstimmung zwischen AG und AN werden daraufhin die dazu anstehenden Aufgaben/Leistungspakete sowie Ergebnisse und Abnahmekriterien definiert, priorisiert und verbindlich schriftlich festgelegt, die der AN dann selbständig bearbeitet bis zur Sach-/Ergebnisvorstellung gegenüber dem AG zur Billigung/Abnahme als vertragsgerechte Leistung.

1.3 Kommunikation

Jedes Projekt verfügt über einen Kommunikationsplan, um die Kommunikation mit allen Beteiligten/ Stakeholdern zu steuern. Bei AN bezieht sich der Begriff „Steuerung“ stets allein auf werks-/sach-/ergebnisorientierte Vorgaben und nicht auf arbeitsorganisatorische, verfahrens-/prozessorientiere Arbeitsanweisungen. Letztere obliegen bei AN gegenüber ihren zur Vertragserfüllung eingesetzten Erfüllungsgehilfen allein den Verantwortlichen/Vorgesetzten des jeweiligen AN.

Die Kommunikation erfolgt ausschließlich über die vertraglich definierten Ansprechpartner des AG und des AN in den vertraglich definierten Formaten und Terminen (z.B. Status-/Scrum-Meetings zweiwöchentlich) und Formen (z.B. Präsenz, Online, Hybrid). Dabei können verschiedene Kommunikationswege und -plattformen genutzt werden, beispielsweise online/virtuell via Webex oder in Präsenz vor Ort.

Kommunikation und Austausch von Informationen ist in einer angemessenen Form innerhalb der Projektdokumentation schriftlich zu protokollieren.

1.4 Tooling & Aufgabenmanagement

Auf Grundlage der spezifischen Anforderungen und Rollenverteilung aus der Leistungsbeschreibung bestimmen sich das Tooling und das Aufgabenmanagement.

Der AG/Product Owner definiert Produktanforderungen eigenständig über das Product Backlog und hat die strategische Produktentwicklung inne. Der AG/Product Owner beschreibt die beauftragten Leistungen in detaillierter Form (z.B. Pflichten/Lastenheft). Das Product Backlog ist die einzige Quelle, aus der der AN den Leistungsauftrag übernimmt. Weitere Konkretisierungen der Leistungsanforderungen sind genau zu dokumentieren.

Für die technisch-begleitende Umsetzung wird die Nutzung des Tools „Jira“ vereinbart, welches seitens AG konfiguriert und zur Vertragserfüllung zur Verfügung gestellt wird. Der AN zieht sich nach dem Pull Prinzip im Rahmen des Vertrages seine Leistungsgegenstände und bearbeitet diese selbständig bis zur Ergebnisrückmeldung, Dokumentation und Ablage in Jira. Der AG verpflichtet sich, dem AN gefilterte Ansichten seiner spezifischen und nach dem Pull Prinzip um Rahmen des Vertrages gezogenen Aufgaben zur Verfügung zu stellen.

Die anstehenden Aufgaben werden seitens AG in Jira nach einer mit dem AN abgestimmten Form (DoR = Definition of Ready) erfasst und im Backlog (Arbeitsvorrat) priorisiert abgelegt. Die als nächstes zu erledigenden Aufgaben stehen im Backlog oben, je weiter eine Aufgabe unten im Backlog steht, desto niedriger priorisiert ist diese.

Der AN ist vertraglich verpflichtet, seine nach dem Pull Prinzip übernommenen Aufgaben in der vorgesehenen Priorisierung abzuarbeiten und den Status gemäß der Kanban Systematik in Jira aktuell und wahrheitsgemäß abzubilden und zu dokumentieren.

Sollte eine Aufgabenstellung unklar/unpräzise oder die gemeinsam festgelegten Regeln der Definition of Readiness nicht eingehalten sein, ist es eigenständige Pflicht des AN, die unklar/unpräzise Aufgabenteile mit entsprechender Rückfrage zur weiteren sachbezogenen/ergebnisorientieren Klärung/Definition i.S.d. § 645 BGB an den AG – genauer den verantwortlichen Autor der Aufgabe – zurückzugeben und dafür die nächst priorisierte klar/präzise Aufgabe zu beginnen.

Dem AN wird Zugriff auf die zur Erfüllung seiner vertraglichen Leistungspflichten erforderlichen Tools nach dem „need to know/must-have-Prinzip“ gegeben bzw. sie ihnen im Rahmen der vertraglichen Pflichten zur Verfügung gestellt.

IT Lösungen und Applikationen im Rahmen PM@BWI:

- Core Client
- Projektmanagement Supporting Platform (JIRA)
- SharePoint Applications
- SharePoint Plattform
- SAP Plattform
- Webex
- Collaboard
- Confluence
- MS Word (MS Office), MS Excel (MS Office), MS PowerPoint (MS Office), E-Mail Service Exchange (Outlook), MS-Project, MS-OneNote, MindJet MindManager.

Projekt- und Prozessverantwortliche stellen für AN den Zugang zu den zur Aufgabenerfüllung relevanten Bereiche und Seiten im Rahmen des technischen Onboardings sicher.

1.5 Dokumentation und Abnahmen

Sofern im Vertrag nichts Anderes geregelt ist, erfolgt die Dokumentation der Leistungen sowie der Ergebnisse durch den AN sowohl in JIRA als auch in weiteren vom Projektverantwortlichen vorgegebenen Systemen in der vom Projekt vorgegebenen Form. Die fachliche/inhaltliche Prüfung der Abnahme(n) erfolgt durch den Projektverantwortlichen. AG und AN haben hierzu den Einbezug der Guidelines des „Software Engineering Frameworks“ in Vertrag/LB vereinbart, die vom AG zur Verfügung gestellt wird.

Der AN stellt die fertiggestellten Vertragsleistungen im Tool JIRA in der Spalte „Abnahme“ für den AG zur Abnahme gemäß der Regelungen des Rahmenvertrages bereit, sobald der AN die vorgegebenen und vereinbarten Ergebnisse erreicht hat.

Der AG als Product Owner testet gemäß der Regelungen des Rahmenvertrages die vereinbarten Abnahmekriterien und bestätigt die Abnahme im JIRA Tool, wenn alle Abnahmekriterien erfüllt sind.

Auftragnehmer/AN können jederzeit nach der Projekt-/Programmmanagementmethodik für die jeweilige Projekt- und Programmmanagement- Phase zu liefernde Ergebnisse hinsichtlich Qualität und Vollständigkeit überprüft werden. Bei Abweichungen des Ist vom Sollzustand können Mängelrügen, Nachbesserungsverlagen o.ä. erfolgen.

1.6 Eskalationswege

Sicherstellung eines Eskalationsmanagements

Das Eskalationsmanagement muss folgende Anforderungen erfüllen:

- Zeitnahe und zielgerichtete Information der Entscheidungsträger
- Erarbeiten von Lösungen insbesondere zu folgenden allgemeinen Themenbereichen:
  - Leistungsstörungen/ Projektabwicklung/ Verzögerungen im Projektablauf
  - Unvorhergesehene Ereignisse
  - Konflikte und Meinungsverschiedenheiten

Ansprechpartner

Der AN muss dedizierte Ansprechpartner zu folgenden Eskalationsstufen benennen:

Eskalationsstufe 1 – Projektverantwortlicher

Eskalationsstufe 2 – Zuständige Vertreter der Bereichsleitung

Eskalationsstufe 3 – Geschäftsleitung

Ablauf einer Eskalation

Mit Bekanntwerden eines Eskalationsthemas informiert der Ansprechpartner der Eskalationsstufe 1 den zuständigen Ansprechpartner der jeweils anderen Partei der Eskalationsstufe 1 per Email über die Einleitung einer Eskalation.
Die Mitteilung sollte dabei folgende Informationen über das Eskalationsthema enthalten:

- Datum des Bekanntwerdens
- Anlass und Beschreibung
- Auswirkungseinschätzung
- Einstufung und Dringlichkeit

Die Ansprechpartner der Eskalationsstufe 1 haben innerhalb einer unter Berücksichtigung der Dringlichkeit und der Auswirkungen angemessenen Frist, mindestens jedoch von fünf (5) Arbeitstagen ab dem Tag des Versands der Eskalationsmitteilung die Aufgabe, Lösungsschritte bzw. eine finale Lösung zu der anhängigen Eskalation unter Einbeziehung der zuständigen Fachabteilungen der Parteien unter Berücksichtigung eines angemessenen Realisierungszeitraums abzustimmen.

Gelingt es der Eskalationsstufe 1 nicht, innerhalb der genannten Frist erste Lösungsschritte bzw. eine finale Lösung zu vereinbaren und/oder deren Umsetzung in die Wege zu leiten, ist nach Ablauf der genannten Frist die Eskalationsstufe 2 von der Eskalationsstufe 1 aktiv einzubeziehen.

Gelingt es auch der Eskalationsstufe 2 nicht, innerhalb einer weiteren Frist von 10 Arbeitstagen Lösungsschritte bzw. eine finale Lösung und/oder Einigung herzustellen, ist als letzte Eskalationsstufe die zuständige Geschäftsleitung beider Parteien einzubinden und über die Eskalation sowie den aktuellen Stand der beidseitigen Bemühungen zur Lösung der Eskalation zu informieren.

Kann auch die Geschäftsleitung beider Parteien keine finale Lösung zu einer anhängigen Eskalation innerhalb weiterer zwanzig (20) Arbeitstage oder einer davon abweichenden, untereinander einvernehmlich vereinbarten Zeitspanne bewirken, ist jede Partei berechtigt, rechtliche Schritte einzuleiten.

Das Recht der Parteien, jederzeit um einstweiligen Rechtsschutz nachzusuchen, bleibt von den vorstehenden Ausführungen unberührt.

Abschluss einer Eskalation

Ist eine Eskalation in beiderseitigem Einvernehmen gelöst, wird das Ende der Eskalation von den zuständigen Ansprechpartnern der Eskalationsstufe 1 in Textform dokumentiert.

Im Nachgang zu einer Eskalation verpflichten sich beide Parteien, die Ursache(n) der Eskalation zu analysieren und nach Möglichkeit Gegenmaßnahmen mit dem Ziel zu vereinbaren, dass sich das betreffende Eskalationsthema und ähnlich gelagerte Eskalationsthemen nicht wiederholen. Die

Parteien werden sich bei der Ursachenanalyse eines Eskalationsthemas in zumutbarem Rahmen unterstützen.

Einstellung einer Eskalation

Sollte eine Eskalation von einer Partei einseitig als beendet erklärt werden, ohne dass die Eskalation von den Parteien einvernehmlich für gelöst und für beendet erklärt wurde, besteht die Verpflichtung zur Beseitigung des die Eskalation auslösenden Eskalationsthemas weiterhin.

Verzeichnisse

Tabellen

Tabelle 1: Meetingarten 5

Abkürzungen

Folgende Abkürzungen werden in diesem Dokument verwendet:

Abkürzung	Bedeutung	Hinweis
AN	Auftragnehmer	Beauftragte Fremdfirma, Externer Dienstleister
AG	Auftraggeber	BWI GmbH

Dokumentenhistorie, Änderungen, Archivierung

Version

Versionshistorie dieses Dokumentes, die aktuellste Version steht an erster Stelle:

Version	Datum	Bearbeiter	Änderungsvermerk zur Vorversion
1.0	13.09.2024	CDO X PM Excellence	Initiale Version

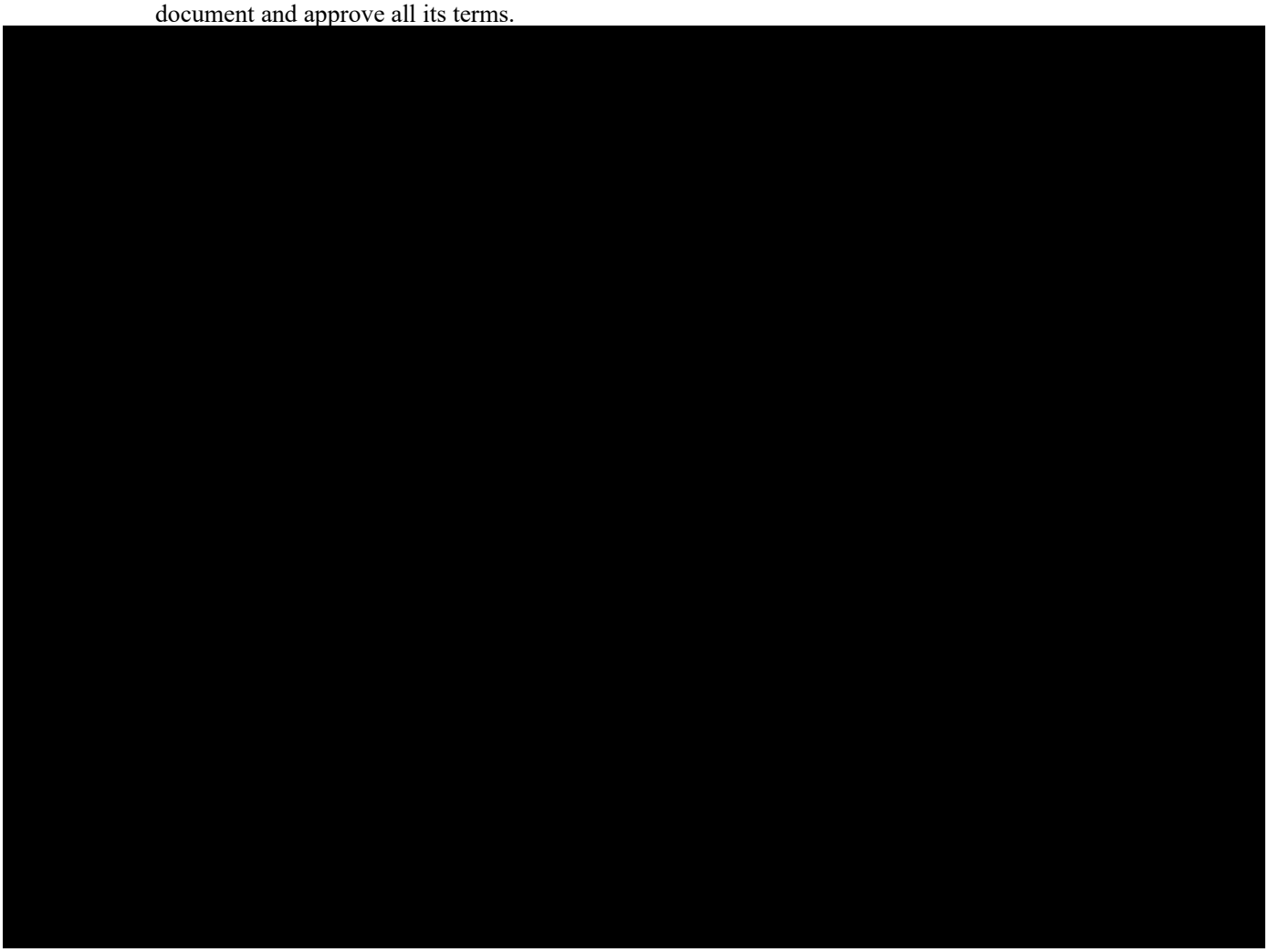
Genderhinweis:

Aus Gründen der besseren Lesbarkeit wird bei Personen- bzw. Rollenbezeichnungen Dokument die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verwendete Sprachform beinhaltet keine Wertung.

Signatures

Number of pages (including this one): 17

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.



BWI
IT für Deutschland

Software Engineering Framework

Software Engineering Framework der BWI und Bundeswehr

Release 2024

Inhalt

Inhalt ... 3
Dokumentenhistorie ... 6
1 Einleitung zum Release 2024 ... 7
1.1 Motivation ... 7
1.2 Abgrenzung ... 9
1.3 Aufbau des Dokuments ... 10
1.4 Änderungen zum Release 2023 ... 12
2 Management Module ... 15
2.1 Software Engineering Process ... 15
2.1.1 Vision ... 15
2.1.2 Inception ... 16
2.1.3 Iterative Realization (DevOps) ... 17
2.1.4 Standard Betrieb ... 18
2.2 Methodology ... 19
2.2.1 Rollen ... 19
2.2.2 Methoden ... 20
2.3 Technology ... 21
2.3.1 Entwicklungsumgebung ... 21
2.3.2 Programmiersprachen ... 22
2.3.3 Externe Komponenten ... 23
2.4 Security & Compliance ... 25
2.4.1 Informationssicherheit ... 25
2.4.2 Datenschutz ... 27
3 Software Engineering Module ... 28
3.1 Discovery & Validation ... 28
3.1.1 Discovery ... 28
3.1.2 Validation ... 29
3.2 Software Design ... 30
3.2.1 Architecture & Design Engineering ... 30
3.2.1.1 Grundsätze ... 30
3.2.1.2 Methoden ... 30
3.2.1.3 Muster ... 31
3.2.1.4 Dokumentationsvorgaben ... 32
3.2.1.5 Weiterführende Architekturrichtlinien ... 32

3.2.2 UX/UI Design 33
3.2.2.1 UX/UI Prozess 33
3.2.3 Sustainable Programming 37
3.3 Coding Guidelines 39
3.3.1 Allgemeine Guideline 40
3.3.2 C# 44
3.3.3 C++ 45
3.3.4 Java 46
3.3.5 JavaScript und TypeScript 48
3.3.6 Kotlin 51
3.3.7 Python 52
3.3.8 Swift 55
3.4 Coding Process 56
3.4.1 Configuration Management 56
3.4.1.1 Configuration Management mit Ansible 57
3.4.2 Version Control 59
3.5 Software Quality & Assurance 62
3.5.1 Software Quality 62
3.5.2 Software Quality Assurance (SQA) 63
3.5.3 Software Quality Control (SQC) 65
3.5.4 Softwaretests (Testing) 66
4 Software Operating Module 72
4.1 Allgemeine Operating Vorgaben 72
4.1.1 Dokumentation 72
4.1.2 Signierung 72
4.1.3 Deployment 72
4.1.4 Inbetriebnahme 73
4.1.5 Operating 73
4.1.6 Monitoring & Reporting 74
4.2 Server-based Applications 75
4.2.1 Deployment 75
4.2.2 Operating 75
4.2.3 Monitoring & Reporting 76
4.3 Cloud Applications 77
4.3.1 Deployment 77
4.3.2 Operating 77

4.3.3 Monitoring & Reporting 77
4.4 Desktop Applications 79
4.4.1 Deployment 79
4.4.2 Operating 79
4.4.3 Monitoring & Reporting 80
4.5 Mobile Applications 81
4.5.1 Signierung 81
4.5.2 Deployment 81
4.5.3 Operating 83
4.5.4 Monitoring & Reporting 83
4.6 AI Applications 85
4.6.1 Vorgaben zu MLOps-Reifegradmodellen 85
4.7 Maintenance & Support 90
4.7.1 Support 90
4.7.2 Maintenance / Wartung 90
4.7.3 Last-Level-Support 91
4.7.3.1 Proaktiver Last-Level-Support 91
4.7.3.2 Prozess 91
4.7.4 Schulungen 97
5 Glossar 98
5.1 Allgemeine Definitionen 98
5.2 Definitionen und Hintergrundwissen zu Software Quality & Assurance 103
5.3 Definitionen zu UX/UI Design 108
5.4 Definitionen zu AI Applications 110
6 Verweise auf andere Dokumente 115
6.1 Anlagen 115
6.2 Mitgeltende Dokumente 115
6.3 Quellen 115

Dokumentenhistorie

Version	Datum	Bearbeiter	Änderungsvermerk zur Vorversion
3.0	29. Januar 2024	BWI GmbH CDO CoE Software Engineering Zentrum Digitalisierung der Bundeswehr	Initiales Release 2024. Änderungen ggü. Release 2023 siehe Abschnitt 1.4.
2.1	01. März 2023	BWI GmbH CDO CS Software Engineering	Aktualisierung des Links zu den BWI Architekturprinzipien und –vorgaben im gesamten Dokument
2.0	30. Januar 2023	BWI GmbH CDO CS Software Engineering	Initiales Release 2023. Änderungen in den entsprechenden Release Notes enthalten.
1.0	16.Mai 2022	BWI GmbH CDO CS Software Engineering	Initiales Release 2022

1 Einleitung zum Release 2024

1.1 Motivation

Dieses Dokument beschreibt eine Zusammenfassung aller Software-Engineering-Standards und Best Practices für Softwareentwickler*innen der BWI und der Bundeswehr als Grundlage für Software Defined Defence mit den Zielen:

- die Software-Engineering-Arbeitsweise zu normieren
- eine hohe Qualität der Arbeitsergebnisse sicherzustellen
- Entwickler*innen effizient und homogen einzuarbeiten
- Projekte beschleunigt zu initialisieren und effizient durchzuführen

Das Software Engineering Framework (SWE Framework) wird veröffentlicht, damit die BWI in Zusammenarbeit mit ihren Entwicklungspartnern eine übergreifende, ganzheitliche und homogene Softwareproduktentwicklung nach Industriestandard und Kundenvorgaben etablieren kann. Es wurde erstmalig 2022 als Diskussionsgrundlage veröffentlicht. Seitdem wird es fortlaufend angepasst, weiterentwickelt und in jährlichen Releases veröffentlicht. Sowohl die inhaltliche Weiterentwicklung als auch die jährliche Veröffentlichung wird als Kooperation zwischen dem Center of Excellence Software Engineering der BWI und dem Zentrum für Digitalisierung der Bundeswehr durchgeführt und von dort aus koordiniert in die weiteren Software-Entwicklungseinheiten der Bundeswehr getragen. Perspektivisch soll das Dokument in einer Vorgabe für Software Engineering münden gemäß CON.8.A11.

Es schafft heute schon Voraussetzungen um:

- kooperative Softwareentwicklungsprojekte zwischen Bundeswehr und BWI durchzuführen,
- Übergaben von Bundeswehr-eigenentwickelter Software im Lebenszyklus an die BWI zu ermöglichen sowie
- SWE-Services der BWI für Softwareentwickler*innen der Bundeswehr mittel- bis langfristig bereitzustellen.

Der Fokus des Dokuments liegt auf einer kurzen und prägnanten Beschreibung der Themen. Auf Tutorials und grundlegende Erklärungen wird - bis auf wenige Ausnahmen - bewusst verzichtet. Es ist ein Informationskatalog „von Profis für Profis“.

Inhaltliche Themen sind:

- Definition fachlicher Leitlinien hinsichtlich Software Engineering.
- Beschreibung von operativen Software-Engineering-Standards und Best Practices.
- Guideline für neue Softwareentwicklungsprojekte und sukzessive Anpassung bestehender Arbeitspraktiken.

Weitere Anregungen begrüßen wir ausdrücklich und stehen für Rückfragen und Unterstützung gerne zur Verfügung!

Inhaltliche Fragen können direkt an die Fachansprechpartner*innen der Kapitel adressiert werden.

Für allgemeine Fragen und die aktuelle Version des SWE Frameworks stehen folgende Funktionspostfächer zur Verfügung: bwi.fp.swe@bwi.de und zdigbwiv1entwicklung@bundeswehr.org.

BWI GmbH/Software Engineering **Zentrum für Digitalisierung der Bundeswehr**

Herausgeber

Carsten Busch, Head of CoE SwE Software Application & Integration, BWI GmbH

Dr. Rolf Hager, Head of CoE Software Engineering, BWI GmbH

LRDir Thomas Schulte, Chief Software Development Officer Bundeswehr, ZDigBw

1.2 Abgrenzung

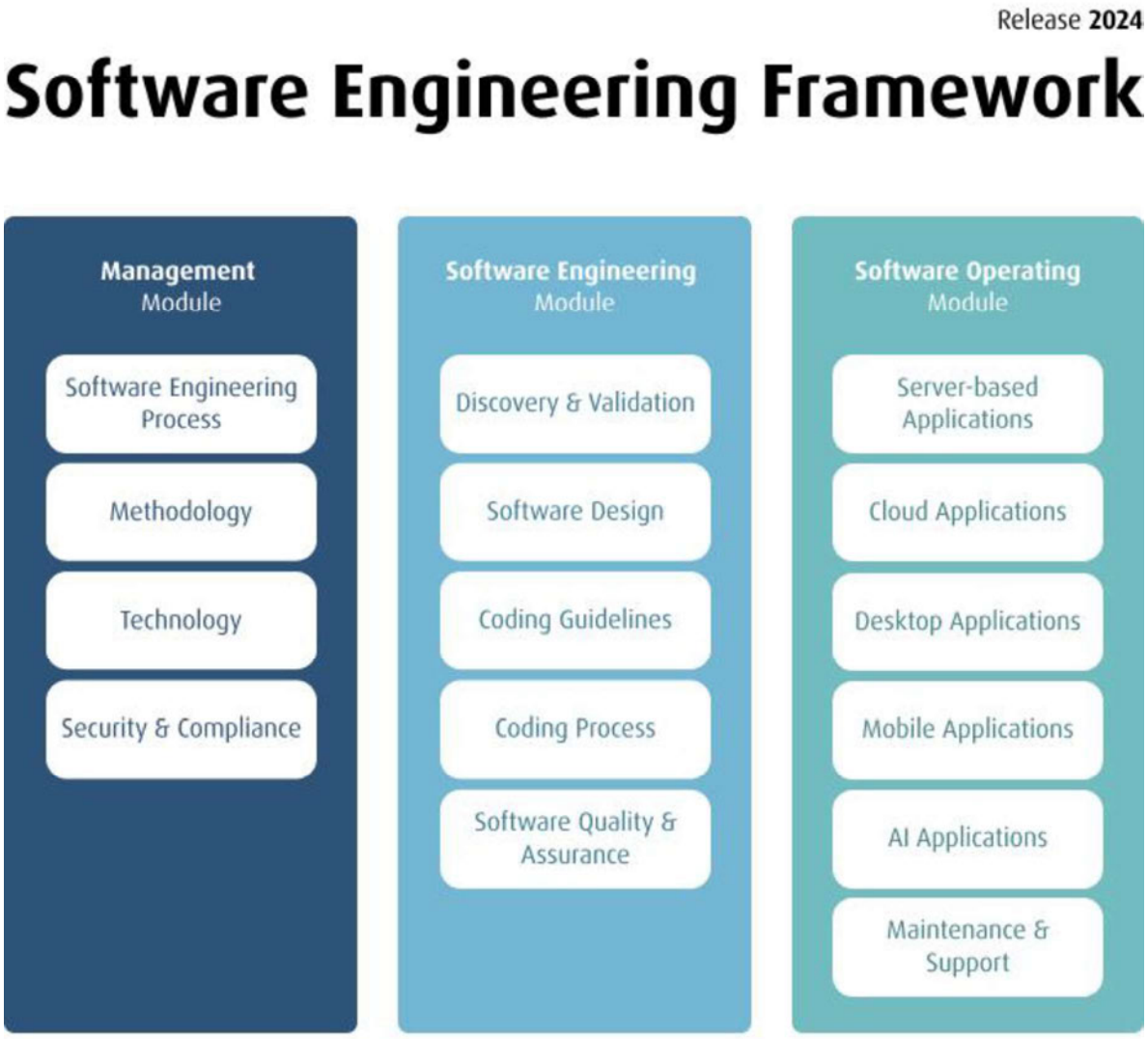
Das SWE Framework orientiert sich grundsätzlich an etablierten Vorgehensweisen und Entwicklungsstandards der Industrie und referenziert diese an den jeweiligen Stellen. Abweichende oder konkretisierende BWI-Spezifika sind entsprechend aufgeführt.

Es gelten folgende Abgrenzungen:

- Das SWE Framework richtet sich in erster Linie an Neuentwicklungen von Software-Produkten. Für Softwarepflege, -wartung und -änderung an bestehenden Eigenentwicklungen, die ursprünglich nicht nach dem SWE Framework entwickelt wurden, sollte geprüft werden, inwiefern das SWE Framework sinnvoll angewendet werden kann. Hierbei müssen die bereits mit dem Kunden abgestimmten Konzepte berücksichtigt werden.
- Softwareentwicklungen im SASPF-Bereich werden über das SWE Framework nicht geregelt. Hier gelten die bestehenden SASPF-Richtlinien.
- Bei prototypischen Anwendungen ist zu prüfen, inwiefern das SWE Framework sinnvoll anzuwenden ist. Im Fall von evolutionären Prototypen greifen die Vorgaben des SWE Frameworks in jedem Fall.

1.3 Aufbau des Dokuments

Das SWE Framework gliedert sich in drei Hauptmodule mit verschiedenen Kapiteln:



Das **Management Module** beinhaltet die Rahmenbedingungen für Software Engineering. Hierzu gehören der Software-Engineering-Prozess, die eingesetzten Methoden und Technologien sowie die Abhängigkeiten zu Richtlinien und Sicherheitsvorgaben innerhalb und außerhalb der BWI.

Das **Software Engineering Module** ist der wesentliche Kern des SWE Frameworks. Das Modul beinhaltet die Standards zur Architektur, zum Design und zur Entwicklung von Software. Zudem werden Methoden zur Anforderungserhebung und Qualitätssicherung beschrieben.

Das **Software Operating Module** beschreibt, wie die eigenentwickelte Software in den BWI-Betrieb überführt und anschließend aus Softwareentwicklungssicht begleitet wird. Dazu zählen Deployment, Operating, Monitoring & Reporting sowie Maintenance & Support. Das Modul beinhaltet ein Kapitel mit allgemeinen Vorgaben sowie Kapitel zu den einzelnen Zielplattformen mit spezifischen Vorgaben.

In allen Kapiteln wird für die Vorgehensweisen und Entwicklungsstandards folgende Notation verwendet:

- [MUSS]: Sagt aus, dass die Vorgehensweise verpflichtend ist.
- [EMPFOHLEN]: Sagt aus, dass sich die Vorgehensweise aus Erfahrungssicht bewährt hat (Best Practice).
- [KANN]: Sagt aus, dass die Vorgehensweise möglich ist (als Alternative zu einer Empfehlung oder als allgemeiner Hinweis).

Projektbedingte Abweichungen von MUSS-Kriterien müssen begründet und dokumentiert werden. Hierzu kann die Checkliste SWE Framework 2024 aus dem Anhang verwendet werden.

Im **Anhang** findet sich folgendes Informations- bzw. Hilfsmaterial:

- *Orientierungshilfe Informationssicherheitsanforderungen*: Dieses Dokument präzisiert die Anforderungen aus Anlage Informationssicherheitsanforderung der BWI in Bezug auf Software Engineering. Zudem werden Handlungsempfehlungen beschrieben, um die Anforderungen zu erfüllen.
- *Checkliste SWE Framework 2024*: Ein Excelsheet, in dem die Inhalte des SWE Frameworks in Checklistenform aufgeführt werden. So können der Erfüllungsgrad der Vorgaben und Empfehlungen erfasst und mögliche Abweichungen begründet werden.
- *Template Aufwandsschätzung*: Dieses Excelsheet kann genutzt werden, um Aufwandsschätzungen für ein Entwicklungsvorhaben im Zuge eines SWAG oder eines Anforderungsworkshops (vgl. Abschnitt Inception) durchzuführen.
- *Template README:* Ein Template, das die im SWE Framework vorgegeben Informationen enthält.
- *EditorConfig* Dateien für die Programmiersprachen Java, JavaScript und Python.

1.4 Änderungen zum Release 2023

An dieser Stelle werden die High-Level Änderungen zusammengefasst. Darüber hinaus sind sämtliche geänderte und neue Kriterien in der Checkliste im Anhang als solche kenntlich gemacht.

Kapitel	Änderung
Allgemein	
	▪ Weiteres Informationsmaterial wurde dem Anhang hinzugefügt: ▫ [4] Template README ▫ [5] Java EditorConfig ▫ [6] JavaScript EditorConfig ▫ [7] Python EditorConfig
Management Module	
Software Engineering Process	▪ Ergänzung zentraler BWI Eingangskanal zur Beauftragung. ▪ Schärfung des Abschnitts *Erstkontakt.* ▪ Überführung in MUSS, EMPFOHLEN, KANN Notation.
Methodology	▪ Auflösung des Unterkapitels *Dokumentation* in die jeweiligen Kapitel.
Technology	▪ Konkretisierung des Abschnitts *Entwicklungsumgebung / Funktionsumfang*, inkl. Ergänzung weiterer Informationen zu DevLabPro. ▪ Detailierung des Abschnitts *Externe Komponenten / Bewertungsleitfaden*. ▪ Verschlankung des Abschnitts *Lizenzrechtliche Vorgaben*.
Security & Compliance	▪ Schärfung hinsichtlich der geltenden Richtlinien und Vorgabedokumente in Abgleich mit dem InfoSichhK. ▪ Ergänzung Einsatz kryptografischer Verfahren / Post-Quantum-Algorithmen. ▪ Neues Unterkapitel *Datenschutz*.
Software Engineering Module	
Discovery & Validation	*Keine Änderungen.*
Architecture & Design Engineering	▪ Anpassung Test Driven Development (TDD) von MUSS auf EMPFOHLEN. ▪ Entfernung NATO Richtlinie, da kein verfügbarer Link vorhanden. ▪ Hinweis: Vollständige Überarbeitung des Kapitels für das Release 2025 geplant.

Kapitel	Änderung
UX/UI Engineering	▪ Ergänzung einer grafischen Darstellung des Prozesses. ▪ Auslagerung der Definitionen ins Glossar. ▪ Anpassung der MUSS, KANN, EMPFOHLEN Kriterien: Entschärfung der MUSS-Kriterien und Umformulierung nach EMPFOHLEN.
Sustainable Programming	▪ Umbenennung des Kapitels (ehemals: *Sustainable Software Engineering*). ▪ Ergänzung Abgrenzung des Begriffs "Nachhaltigkeit". ▪ Ergänzung weiterer optionaler Aktivitäten zur Minimierung des Energieverbrauchs.
Coding Guideline / Allgemeine Guideline	▪ Allgemeine Guideline ▫ Grundlegende Überprüfung und Anpassung aller Kriterien. ▫ Auslagerung der EditorConfigs in die sprachspezifischen Kapitel. ▫ Aufnahme Clean Code Best Practices. ▪ C# ▫ Aufnahme Empfehlung hinsichtlich zu nutzender IDE. ▪ C++ ▫ Aufnahme zu nutzende IDE und Testing Frameworks. ▪ Kotlin ▫ IDE Unterscheidung zwischen Android und anderen Projekten. ▫ Aufnahme Ktlint. ▫ Aufnahme Testing. ▪ Swift ▫ Aufnahme Formatierung. ▫ Aufnahme Testing. ▪ Java ▫ Aufnahme Testing. ▪ JavaScript und TypeScript ▫ Umbenennung des Kapitels (ehemals nur JavaScript). ▫ Ergänzung BWI React Starter Projekt. ▫ Aufnahme Tailwind. ▫ Aufnahme Vitest. ▫ Aufnahme Scaffolding.

Kapitel	Änderung
	▪ Python ▫ Ergänzung Mamba. ▫ Ergänzung automatisiertes Testen mit mypy. ▫ Ergänzung Network Programming mit Twistet.
Configuration Management	▪ Neues Unterkapitel *Configuration Management mit Ansible*. ▪ Ergänzung optionale Aktivitäten bzgl. Konfigurationsdateien.
Version Control	▪ Einheitliche Umbenennung von master zu main. ▪ Schärfung Regeln zu LFS. ▪ Ergänzung und Konkretisierung im Abschnitt *Merge Request/Code Review*. ▪ Ergänzung scaled-trunk-based Ansatz.
Software Quality & Assurance	▪ Ergänzung des Abschnitts *Hinweise zu Testfällen*. ▪ Auslagerung der Definitionen und Hintergrundwissen ins Glossar.
Software Operating Module	
Allgemeine Operating Vorgaben	▪ Ergänzung des Abschnitts *Inbetriebnahme*. ▪ Konkretisierung der Abschnitte *Dokumentation, Deployment, Operating, Monitoring & Reporting*.
Server-based Applications	*Keine Änderungen.*
Cloud Applications	▪ Zusammenfassung der Vorgaben im Abschnitt *Monitoring & Reporting*. ▪ Konkretisierung der Aktivitäten im Abschnitt *Deployment*.
Desktop Applications	▪ Zusammenfassung der Vorgaben im Abschnitt *Monitoring & Reporting* (analog zu Cloud). ▪ Ergänzung Richtlinien zur Paketierung und Paketierungsstrategie.
Mobile Applications	*Keine Änderungen.*
AI Applications	▪ Neues Kapitel.
Maintenance & Support	▪ Neues Unterkapitel *Last-Level-Support*.

2 Management Module

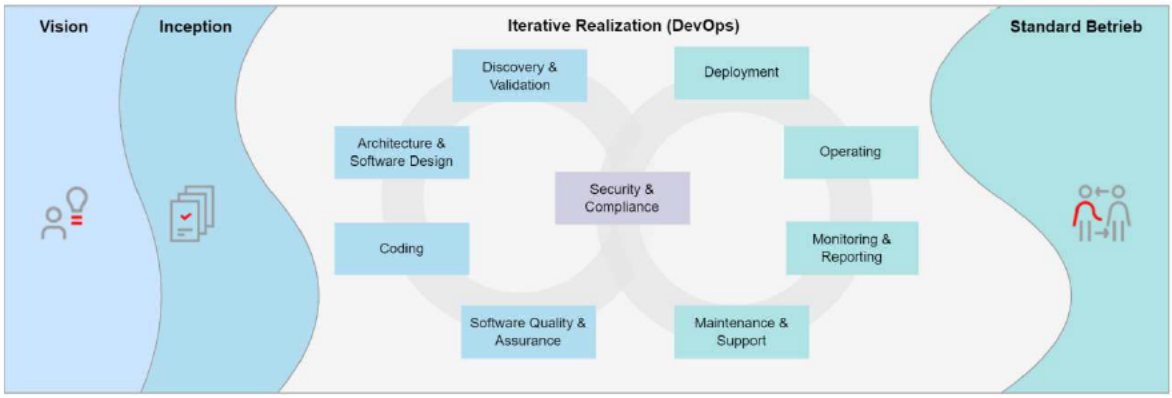
Das Management Module beinhaltet die Rahmenbedingungen für Software Engineering. Hierzu gehören der Software-Engineering-Prozess, die eingesetzten Methoden und Technologien sowie die Abhängigkeit zu Richtlinien und Sicherheitsvorgaben innerhalb und außerhalb der BWI.

2.1 Software Engineering Process

*Ansprechpartner*innen: Janina Moser, BWI; Dominik Röser, ZDigBw*

Dieses Kapitel zeigt, wie die einzelnen Module des Software Engineering Frameworks im Zusammenhang stehen und wie DevOps, das Entwicklungs- und Betriebsparadigma, in den Gesamtprozess eingebettet ist. Es beschreibt außerdem, wie ein Software-Engineering-Vorhaben initiiert wird und welche Voraussetzungen erfüllt sein müssen, damit die Softwareproduktentwicklung in der BWI starten kann.

Der Software-Engineering-Prozess beinhaltet folgende Schritte, die in den nachfolgenden Kapiteln erläutert sind:



2.1.1 Vision

[MUSS]: Eingangskanal

Mit einer neuen Kundenanfrage beginnt der Software-Engineering-Prozess. Innerhalb der BWI wird eine Anfrage für Software-Engineering-Leistungen über die standardisierte Seite Center of Excellence Ressourcenmanagement oder direkt über Dynamo gestellt. Anschließend wird das Vorhaben in das SWE-Auftragsbuch überführt und ein Termin für den Erstkontakt vereinbart.

[MUSS]: Erstkontakt

Der Erstkontakt ist ein Gespräch, bei dem der Kunde eine erste Übersicht über das Vorhaben vorstellt:

- Grobe fachliche Anforderungen: Was soll entwickelt werden? Was ist der zu erwartende Mehrwert?

- Kontext: In welchem Kontext steht das zu entwickelnde Produkt? Geht es um eine Neu- oder Weiterentwicklung eines Legacy-Produkts oder um die Umsetzung einer gänzlich neuen Lösung?
- Machbarkeitsanalyse: Hat die Anfrage einen Software-Engineering-Bezug? Ist die Anfrage umsetzbar?
- Wiederverwendbarkeit: Gibt es bereits einen Prototypen oder Komponenten zu diesem Vorhaben? Falls ein Prototyp existiert, ist dieser SWE Framework-konform, damit auf dessen Basis weiterentwickelt werden kann oder muss neu entwickelt werden?
- Technische Einordnung des Einsatzgebiets: In welchem Systemumfeld soll das Produkt eingesetzt werden? Gibt es dazu entsprechende Sicherheitsanforderungen? Wie viele Nutzer werden erwartet? In welcher Zielumgebung soll das Produkt betrieben werden? Gibt es bereits bekannte essentielle Schnittstellen?
- Zeitlicher Rahmen: Wann soll das Vorhaben starten? Welche weiteren zeitlichen Parameter gibt es? Welche Priorität/Dringlichkeit hat das Vorhaben? Wann wird eine einsatzfähige Lösung erwartet?
- Ansprechpartner definieren: Wer sind die zentralen Ansprechpartner? (Im Bw-Umfeld ist die frühzeitige Klärung des IT-SVEB (IT-Service-Verantwortlicher Bw oder IT-Service Owner) empfohlen.) Wer wird das Vorhaben z. B. als Subject Matter Expert/Advisor (siehe Kapitel Methodology) begleiten? Wer ist der Auftraggeber?
- Budget: Gibt es ein Budget bzw. einen Auftrag (Lieferverpflichtung) für Entwicklung und den Betrieb? Wer finanziert das Vorhaben?

2.1.2 Inception

Das Ziel der Inception Phase ist eine Abschätzung der Anforderungen, des Scopes und der Rahmenbedingungen der jeweiligen Anfrage zu erstellen, um das Softwareprodukt ganzheitlich entwickeln zu können. Die Abschätzung gliedert sich in zwei Teile:

[EMPFOHLEN]: Erster Schritt: Scientific Wildly Aimed Guess (SWAG)

- Eine einfache Schätzung basierend auf der Erfahrung der Software-Engineering-Expert*innen.
- Minimaler Invest: Zeitaufwand von etwa einer Stunde.
- Diese erste Abschätzung darf eine Unschärfe von 100% aufweisen.

[MUSS]: Im Anschluss: Anforderungsworkshop

Ein Anforderungsworkshop von zwei bis drei Tagen wird durchgeführt. Sofern ein SWAG vorhanden ist, werden die SWAG Ergebnisse während des Anforderungsworkshops präzisiert. Ziel des Anforderungsworkshops ist, je nach Vorhaben, Anforderungen gemeinsam mit dem Kunden zu erkennen, zu präzisieren und zu bewerten. Dabei können Antworten zu den nachfolgenden Punkten erarbeitet werden, um aus Software-Engineering-Sicht die benötigten Mitarbeitenden sowie benötigte Technik zu identifizieren. Bei dieser Ausarbeitung sollten Mitarbeitende des späteren Projektteams von Anfang an maßgeblich beteiligt sein. Die Verrechnung und Beauftragung findet gemäß BWI-Vorgaben in Abstimmung mit dem Account Management statt.

- Entwurf eines Grob-Konzepts: Hierbei sollten die definierten Anforderungen nicht zu feingranular sein und keine technische Lösung vorwegnehmen.

- Prüfung von Standardsoftware oder bereits vorhandene Eigenentwicklungen als mögliche Lösungsalternative (Prüfung auf COTS / MOTS).
- Erstellung einer High-level-Architektur / Infrastruktur.
- Anwendung von Spikes / Rapid Prototyping / Wireframes.
- Anlegen erster Epics / Stories.
- Durchführung von Design Sprints.
- Abschätzung der Aufwände zur Erstellung des Informationssicherheitskonzepts InfoSichhK und des Datenschutzkonzepts DSK.
- Eingrenzung des Vorgehensmodells: Abhängig von den Anforderungen, insb. den Sicherheitsanforderungen, kommen unterschiedliche Methoden zum Einsatz. Agile Vorgehensweisen, wie im Kapitel Methodology beschrieben, werden angestrebt.
- Identifikation von Abhängigkeiten zu anderen Systemen, Netzübergängen und Sicherheitsdomänen / Erstellung eines Abhängigkeitsgraphen.
- Planung Software Development Environment (siehe Kapitel Technology).
- Nutzung des verfügbaren Templates für die Aufwandsschätzung zur Übermittelung an den Kunden im Verweise auf andere Dokumente.
- Erarbeitung der Qualitätsziele (siehe Kapitel Architecture & Design Engineering).

[MUSS]: SWE Auftragsbacklog

Das Vorhaben wird im SWE-Auftragsbuch kontinuierlich aktualisiert. Die Priorisierung geschieht in Abhängigkeit von den folgenden Punkten:

- Vorgegebene Projektpriorisierung durch die BWI.
- zeitlicher Rahmen sowie Dauer des Vorhabens.
- Umfang des zu entwickelnden Produkts.
- Dringlichkeit.
- Verfügbarkeiten der für das Vorhaben relevanten Mitarbeitenden.

2.1.3 Iterative Realization (DevOps)

[MUSS]: Umsetzung nach agilem Vorgehen

Der Fokus dieser Phase liegt auf der iterativen und inkrementellen Produktentwicklung. In der BWI startet diese, sobald SWE den Auftrag zur Umsetzung des Vorhabens gemäß BWI-Prozessen und Vorgaben erhält.

- Zu Beginn:
  - Auswahl eines bereits eingespielten Teams oder Aufbau eines neuen Teams (Staffing je nach Verfügbarkeit und Know-how durch BWI/Bw/Externe) einschließlich der Software-Engineering-Expert*innen, die idealerweise bereits das SWAG und den Anforderungsworkshop durchgeführt haben sowie
  - Abstimmung über das Vorgehensmodell im Team (siehe Kapitel Methodology) inkl. rechtzeitiger Planung, Anmeldung neuer betrieblicher Anforderungen bei den jeweiligen Operations Services.

- Start der agilen Produktentwicklung mit regelmäßigen Releases. In Ausnahmefällen können auch andere Vorgehensweisen vereinbart werden.
- Parallele Bearbeitung der Aktivitäten aus den Modulen Software Engineering sowie Software Operating.
- DevOps (als eine cross-funktionale Team-Besetzung aus den erforderlichen Bereichen (z. B. Dev und Ops) sowie die obligatorische Berücksichtigung der Security-Aspekte) als Entwicklungs- und Betriebsparadigma. Somit ist sichergestellt, dass alle Compliance- und Sicherheitsanforderungen im gesamten Lifecycle erfüllt werden.
- Regelmäßiges Einholen von Feedback von allen relevanten Stakeholdern und Berücksichtigung bei der Umsetzung (Inspect & Adapt z. B. im Sprint Review).
- Kontinuierliche Anpassung des Product Backlogs auf Basis des Feedbacks, der Rahmenbedingungen des Vorhabens und neuer oder veränderter Anforderungen (funktional sowie nicht-funktional).

2.1.4 Standard Betrieb

[KANN]: Indikatoren für die Überführung in den Regelbetrieb:

- Feature-complete.
- Qualitätsziele erfüllt.
- Beta-Phase abgeschlossen.
- Backlog geleert.
- Abnahmetest durch den Kunden abgeschlossen.
- Produktionsfreigabe (durch den Kunden) erteilt.
- Schwachstellen, die ggf. noch im Softwareprodukt enthalten sind, werden akzeptiert.
- Dokumentation abgeschlossen.
- 3rd Level Supportteam definiert und Supportprozesse geklärt.

Sobald das Softwareprodukt in den Regelbetrieb überführt wird, tritt eine reine Betriebsphase ein. In der BWI wird dieser Betrieb hauptverantwortlich durch die Betriebseinheit Application Management durchgeführt. Hierbei wird der 3rd Level Development Support weiterhin von einem Teil des ursprünglichen Entwicklungsteams bereitgestellt. Ferner werden bei einer neuen Sicherheitslücke (in einer externen Komponente oder im eigenentwickelten Source Code) Entwicklungsleistungen bereitgestellt, um diese Sicherheitslücken umgehend zu entfernen gemäß CON.8.A8.

Retirement bzw. Ausphasung: Ist der "End of Life"-Zustand erreicht, wird der Betrieb eingestellt und ggf. eine Migration in eine nachfolgende Software durchgeführt. Die Software sowie alle Dokumentationen werden archiviert.

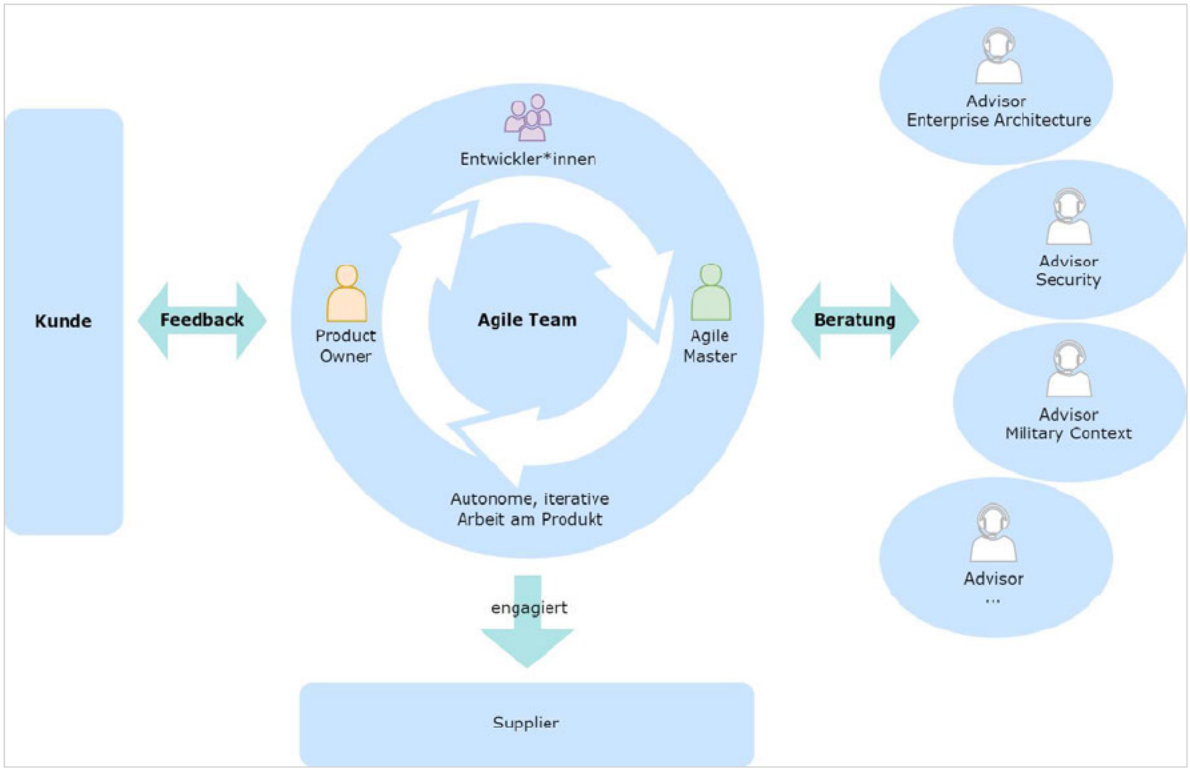
2.2 Methodology

Ansprechpartner: Christoph Winkler , BWI

Zum Start eines Software-Engineering-Vorhabens muss eine geeignete Methodenauswahl getroffen werden. Dies wird im gesamten Team diskutiert und abgestimmt. Die Methode muss dabei zur jeweiligen Problemstellung bzw. den Anforderungen passen. Im Rahmen des Software Engineering Frameworks wird Softwareentwicklung nach agilen Frameworks (z. B. Scrum, Kanban) empfohlen.

2.2.1 Rollen

[MUSS]: Im agilen Umfeld sind folgende Rollen und Interaktionen gemäß CON.8.A1 relevant:



Rolle	Beschreibung
Kunde	Kunde begleitet die Entwicklung fortlaufend und stellt ggf. einen SME (s. u.) oder PO.
PO	Der Product Owner ist der Produktverantwortliche und soll den Business Value des Produktes maximieren. Er entscheidet über Features und priorisiert diese in der Umsetzung. Wenn der PO nicht durch den Kunden gestellt werden kann, wird ein PO vom Auftragnehmer gestellt, dieser wird Proxy Product Owner genannt.

Rolle	Beschreibung
Agile Master	Der agile Master als agiler Coach optimiert die Arbeitsweise des Teams und wirkt als Servant Leader.
Agile Team	Das agile Team besteht cross-funktional aus allen benötigten Fähigkeiten, um autonom Entscheidungen treffen zu können. Das Team kann sich Expertise des SME oder Advisors einholen und umsetzen.
Advisor bzw. SME	Der Advisor bzw. Subject Matter Expert stehen dem Team für spezielle Themen zur Verfügung und können punktuell unterstützen. Jede Umsetzungsentscheidung bleibt eine Entscheidung des Teams.
Supplier	Dienstleister können für die Umsetzung vom Team engagiert werden.

2.2.2 Methoden

[MUSS]: Auswahl des Vorgehensmodells gemäß CON.8.A2 und CON.8.A16:

BWI-eigene Methoden

Alle Projekte der BWI müssen die BWI-weit gültige Projektmanagement-Methodik PM@BWI anwenden sowie, abhängig vom Projekt, weitere Praktiken wie EPDF@BWI bedienen. Im Kontext von PM@BWI können ergänzende Hilfestellungen im BWI-internen Agile Playbook eingesehen werden. Zu den einzelnen Methoden existieren eigene Dokumentationen, die unter folgenden Links eingesehen werden können: EPDFund PM@BWI .

Scrum

Bei einer Entscheidung für die Anwendung des Scrum Frameworks muss sich an der aktuellen Fassung des Scrum Guides orientiert werden. Eine Abweichung hiervon wird nicht angestrebt. Die aktuelle Fassung des Scrum Guides findet sich unter: Scrum Guide 2020

Spezielle Ausprägungen:

Abhängig von den Anforderungen an das Software-Engineering-Vorhabens und insbesondere in sicherheitskritischen Bereichen könnten spezielle Ausprägungen wie z. B. SafeScrum (nicht zu verwechseln mit dem agilen Skalierungsmodell SAFe) in Erwägung gezogen werden [Han18].

Kanban

Die Kanban Methode setzt den Fokus auf die Durchsatzoptimierung der Arbeit, d.h. auf eine schnelle und effiziente Bearbeitung von Aufgaben. Bei der Umsetzung soll auf die Einhaltung der Prinzipien und Praktiken nach David Anderson geachtet werden. Eine Erklärung für Kanban findet sich in dem offiziellen Leitfaden zur Kanban-Methode .

V-Modell (XT)

Das V-Modell ist eine geschützte Marke der Bundesrepublik Deutschland und wird daher häufig im Behördenumfeld (z. B. auch Bw) genutzt. Die aktuelle Fassung des V-Modells kann auf der Homepage des CIO des Bundes eingesehen werden: V Modell XT.

2.3 Technology

Ansprechpartner: Fabian Angelstorf, BWI; Norman Nemitz, BWI

Die eingesetzte Technologie spielt eine entscheidende Rolle für den Erfolg des Software Engineerings. Einerseits werden geeignete Entwicklungsumgebungen benötigt, um effiziente und sichere Software entwickeln zu können. Andererseits beeinflussen die eingesetzten Technologien, wie Programmiersprachen und externe Komponenten, das zu liefernde Produkt.

2.3.1 Entwicklungsumgebung

Eine mandantenfähige, skalierbare und sichere Softwareentwicklungsumgebung stellt grundlegende Funktionen zur Software-Entwicklung zentral bereit und bietet Entwicklern so eine verlässliche Grundlage für die effiziente Entwicklung hochwertiger Softwarelösungen. In der BWI wird eine entsprechende Entwicklungsumgebung gemäß BSI-Grundschutz (v.a. CON.8.A3, sowie CON.8.A17 bis CON.8.A19) durch den Service Software Development Environment (SDE) (Kontakt: bwi.fp.buenosdeaas@bwi.de) bereitgestellt. Durch die Erfüllung der Anforderungen des BSI-Grundschutz trägt die Entwicklungsumgebung dazu bei, Manipulationen, Verlust und den unautorisierten Abfluss von Quellcode zu verhindern. Standardisierte Vorgehensweisen sichern und optimieren darüber hinaus den Software-Erstellungsprozess und mindern potenzielle Kompatibilitätsprobleme.

Funktionsumfang

Der SDE-Service beinhaltet in der ersten Ausbaustufe die folgenden Funktionen, Werkzeuge und Prozesse. In Klammern angegeben sind die Produkte, für die bereits ein Rahmenvertrag vorhanden ist:

- Code Versionierung gemäß CON.8.A10 (GitLab Ultimate).
- Product Building (GitLab Runner).
- Statische Codeanalyse (Sonarsource Sonarqube).
- Artefaktspeicher / Repositorymanagement (Sonatype Nexus Repository Pro / Harbor).

Folgende Funktionen, Werkzeuge und Prozesse werden in weiteren Ausbaustufen des SDE-Services bereitgestellt:

- Komponentenanalyse für Schwachstellen und Lizenzen gemäß CON.8.A20.
- Qualitätssicherung und Testwerkzeuge (Keysight Eggplant).
- Monitoring & Reporting.
- zentral bereitgestellte IDE-Lizenzen.
- Bereitstellung von Entwickler-Clients.
- weitere Standardtools für Entwicklung und entwicklungsnahe Tätigkeiten (z. B. Wireframe).

Sollten weitere Funktionen, Werkzeuge oder Prozesse benötigt werden, können die Anforderungen mit dem SDE-Service abgestimmt werden.

Für die SDE werden unterschiedliche Ablaufumgebungen angeboten, die auf dem o.g. Technologie-Stack basieren. Aktuell in der Planung und Entwicklung sind die folgenden Umgebungen:

- SDE@DevLabPro für die Entwicklung und Bereitstellung von Softwareartefakten in einem geschützten, isolierten Bereich, erreichbar über das Internet (aktueller Stand 01/2024: im Aufbau).
- SDE@EwS (pCloudBw) für die Entwicklung und Bereitstellung von Softwareartefakten auf der pCloudBw (aktueller Stand 01/2024: im Pilotbetrieb).

Vorgaben

- [MUSS]: Für jedes Software-Engineering-Vorhaben muss eine geeignete Softwareentwicklungsumgebung verwendet werden. Generell steht hierfür der SDE-Service zur Verfügung.
- [MUSS]: Die Nutzung eines CVE-Scanners ist vor Auslieferung der Artefakte verpflichtend. Hier müssen auch externe Komponenten mitgeprüft werden.
- [EMPFOHLEN]: Die Nutzung eines Antiviren-Scanners (nicht Teil des Funktionsumfangs der SDE) ist vor Auslieferung der Artefakte empfohlen.

2.3.2 Programmiersprachen

Bei Neuentwicklungen werden vorrangig folgende Programmiersprachen in Abhängigkeit softwaretechnischer Anforderungen genutzt. Die entsprechenden Leitfäden sind bei der Entwicklung zu berücksichtigen:

- Java (Coding Guideline in Kapitel Java)
- C# (Coding Guideline in Kapitel C#)
- JavaScript / TypeScript (Coding Guideline in Kapitel JavaScript und TypeScript)
- Kotlin für die Entwicklung von Android Apps (Coding Guideline in Kapitel Kotlin)
- Swift für die Entwicklung von iOS und MacOS Apps (Coding Guideline in Kapitel Swift)
- Python (Coding Guideline in Kapitel Python)

Je nach Anforderungen können weitere Programmiersprachen unterstützt werden, wie beispielsweise:

- C++ (Coding Guideline in Kapitel C++)

Die Anzahl genutzter Programmiersprachen sollte allerdings so klein wie möglich bleiben.

Die Liste der Programmiersprachen wird auf Basis der Veränderungen im Bereich der Softwareentwicklung kontinuierlich aktualisiert.

2.3.3 Externe Komponenten

Der Einsatz von externen Komponenten muss sorgfältig bewertet werden gemäß CON.8.A6. Generell muss im Vorfeld die Notwendigkeit für einen Einsatz geprüft werden. Zudem müssen die lizenzrechtlichen Vorgaben beachtet werden.

Bewertungsleitfaden

Zur Bewertung von externen Komponenten müssen folgende Kriterien herangezogen werden:

- Einordnung und Eignung für den eigenen Use-Case:
  - Ist der Einsatz der Komponente notwendig?
- Vertrauen in den Herausgeber:
  - Ist der Herausgeber bekannt?
  - Ist der Herausgeber mit einem Staat im Sinne von § 13 Abs. 1 Nr. 17 Sicherheitsüberprüfungsgesetz - SÜG assoziiert?
- Sicherheit der Komponente:
  - Sind Sicherheitslücken oder Schwachstellen bekannt?
- Verbreitung der Komponente:
  - Kommt die Komponente in anderen eigenen Produkten zum Einsatz?
- Häufigkeit der Releases und Zeitpunkt des letzten Releases:
  - Wird die Komponente noch aktiv weiterentwickelt?
  - Ist zu erwarten, dass die Komponente langfristig weiterentwickelt wird?
  - Werden aufgedeckte Sicherheitslücken geschlossen?
  - Wie lange wird die Komponente noch supportet?
- Aufwandseinschätzung der Eigenentwicklung gegenüber Integrations- und Anpassungsaufwand.
- Lizenz-Modell:
  - Darf die Komponente überhaupt verwendet werden?
  - Welche Einschränkungen gehen mit der Nutzung einher?
- Sicherstellung der Digitalen Souveränität:
  - Erzeugt der Einsatz eine einseitige Abhängigkeit zu einzelnen Herstellern (Vendor Lock-In)?

Zur Steigerung der Harmonisierung der Eigenentwicklungen sind zudem Komponenten zu bevorzugen, die bereits in anderen Eigenentwicklungen zum Einsatz kommen.

Die Einführung eines Tools zur transitiven Komponentenanalyse von Schwachstellen und Lizenzen befindet sich in Pilotierung (Stand 01/24). Dadurch wird die toolgestützte Durchsetzung der Vorgaben ermöglicht.

Lizenzrechtliche Vorgaben

Sowohl beim Verwenden von zusätzlichen Hilfsmitteln als auch bei Einsatzmitteln ist auf die Lizenzen der eingesetzten Produkte zu achten.

- [MUSS]: Die Produkte dürfen nur entsprechend ihrer Lizenzbedingungen eingesetzt werden.
- [MUSS]: Es dürfen nur Artefakte verwendet werden, deren Herkunft eindeutig ist. Durch das verpflichtende Vorhalten einer Software Bill of Material (SBOM) wird auch dem Auftraggeber jederzeit transparent dargestellt, welche Komponenten aktuell verwendet werden (Compliance-Sichtbarkeit). Die SBOM muss die formellen und fachlichen Vorgaben gemäß BSI-Richtlinie TR-03182-2 erfüllen. (siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03183/BSI-TR-03183-2.pdf)
- [MUSS]: In den Umgebungen der BWI muss für die Nutzung von Eigenentwicklungen und Entwicklungswerkzeugen der Freigabeprozess des CERT genutzt werden (vgl. CERT BWI | FAQ (bwi-intranet.de).
- [MUSS]: Innerhalb der BWI müssen die Vorgaben des Lizenzmanagements gemäß der Verfahrensanweisung eingehalten werden. Dazu muss bei der Beschaffung von Softwarelizenzen und bei dem geplanten Einsatz von Open Source Softwareprodukten der Software-Asset Management Service der BWI zwingend involviert werden (Kontakt: bwi.fp.Lizenzmanagement@bwi.de).
- [MUSS]: Bei der Beschaffung von lizenzpflichtigen Produkten sind die geltenden Beschaffungsregelungen zu beachten.
- [MUSS]: Bei der Beschaffung von lizenzpflichtigen Produkten sind als öffentliche Auftraggeberin im Sinne des § 99 Nr. 2 GWB die gesetzlichen Regeln des Vergaberechts bei der Erteilung von Aufträgen an Geschäftspartner zu beachten. Daher müssen Produkte oberhalb des EU-Schwellenwerte im Rahmen eines europaweiten Vergabeverfahrens vergeben werden (EU-Schwellenwert 2024/2025: 221.000 €).
- [MUSS]: Wenn Open Source genutzt werden soll, muss die Nutzung vor dem Entwicklungsstart zwischen dem Auftraggeber und der BWI vereinbart werden.
- [EMPFOHLEN]: Der Einsatz von Open Source ist zu bevorzugen.

Das Mitwirken in Open Source Communities befindet sich noch in Klärung. Aktuell ist ein Mitwirken nur mit expliziter Genehmigung gestattet.

2.4 Security & Compliance

In allen Phasen des Software-Engineering-Prozesses müssen sämtliche Compliance, Datenschutz- und Sicherheitsanforderungen eingehalten werden.

2.4.1 Informationssicherheit

Ansprechpartner: Burkhard Pietsch, BWI; Günter Liehl, BWI

[MUSS]: Konkret müssen folgende Themenbereiche bearbeitet werden:

- Informationssicherheit: Jedes Softwareprojekt benötigt zwingend ein InfoSichhK (inkl. Bedrohungsmodellierung gemäß CON.8.A12 und CON.8.A21). Dafür existiert in der BWI die Richtlinie zum Management von Informationssicherheit, insbesondere die Konkretisierungen in der Anlage Informationssicherheitsanforderungen. Da die Richtlinie nicht immer den Anforderungen einer zu entwickelnden Software entspricht, müssen bei Bedarf frühzeitig Ausnahmegenehmigungen bei CISO beantragt werden (z. B. bei der Nutzung von GPUs in Containern).
  Unterstützend für das InfoSichhK kann die Orientierungshilfe zur Informationssicherheit im Verweise auf andere Dokumente genutzt werden, in der die relevanten Anforderungen mit Bezug auf Software Engineering hervorgehoben werden gemäß CON.8.A5 .
  Das InfoSichhK deckt, abhängig von der jeweiligen Zielumgebung, die folgenden Richtlinien ab:
  - BSI IT-Grundschutz (CON.8)
  - BSI Technische Richtlinien (bei Bedarf)
  - BSI Mindeststandards Bund

- VS-Einstufung: Generell muss immer eine Einstufung der Schutzbedürftigkeit der Projektinhalte im Rahmen des InfoSichhK vorgenommen werden. Die daraus resultierenden Vorgaben werden in der Regel durch die Absicherung der zugrundeliegenden Infrastruktur und nicht durch die zu entwickelnde Software erfüllt. Wenn die Infrastruktur diese Anforderungen nicht erfüllt, müssen softwareseitig entsprechende Vorkehrungen getroffen werden (z. B. die Verschlüsselung der gespeicherten Daten auf einer unverschlüsselten Datenbank außerhalb des IT-SysBw).
- Vorgaben für CVEs für alle eingesetzte Artefakte.
- Betrachtung der verfügbaren und zugelassenen Post-Quantum-Algorithmen für den jeweiligen Use Case.
- Weitere Richtlinien, die für den jeweiligen Anwendungsfall bzw. das Umfeld relevant sind, sind unabhängig vom SWE Framework zu betrachten und werden hier nicht gesondert aufgeführt.

Die folgenden aktuellen Richtlinien für sichere Softwareentwicklung sind relevant und sollten beachtet werden:

- Architekturvorgaben und -prinzipien der BWI :
  - AP03: Automatisierung.
  - AP05: Benutzbarkeit.
  - AVEA01; Anforderungsgetriebene Entwicklung.
  - AVEA03: Verwendung von Standards und einheitlichen Methoden.
  - AVEA05: Sicherstellung von Benutzerfreundlichkeit.
  - AVEA13: Skalierbarkeit von Anwendungen und IT-Plattformen.
  - AVEA16: Nutzung von Interimslösungen.
  - AVIS03: „Security by Design“ im Lebenszyklus von Services, IT-Systemen und Produkten.
  - AVIS04: Sichere Systemgrundkonfiguration („Security-by-Default“).
  - AVIS08: Einsatz kryptografischer Verfahren.
  - AVSA08: Nutzung von Identity & Access Management-Services.
  - AVISA01: Nutzung von einheitlichen und quelloffenen Formaten für den Austausch von Daten und Informationen.
  - AVISA02: Nutzung standardisierter Zeichensätze und –kodierungen.
  - AVISA04: Einsatz von Standards bei Geodaten und Geodatenservices.
  - AVTA01: Verfolgung des Cloud-First-Ansatzes.
  - AVTA02: Virtualisierung von Anwendungen und IT-Plattformen.
  - AVTA10: REST-basierte Schnittstellen der Anwendungen und Plattformen.
  - AVTA15: Nutzung von standardisierten Programmiersprachen und Entwicklungsumgebungen für die serverseitige Anwendungsentwicklung.
- Umsetzungsplan Bund .
- Zentrale Dienstvorschriften der Bw, insbesondere:
  - A-960/1 "Informationssicherheit".
  - A-1130/2 VS-NfD „Militärische Sicherheit in der Bundeswehr - Verschlusssachen“.

Das Ziel ist, auf bekannte Bedrohungsszenarien vorbereitet zu sein, um Datenverluste, unbefugte Zugriffe, Flooding-Attacken usw. zu verhindern. Als Grundlage dienen die Richtlinien der OWASP Foundation. Insbesondere für sicheres Software Engineering dienen folgende Konkretisierungen als Orientierung:

- OWASP Application Security Verification Standard - Web Applikationen.
- OWASP Mobile Application Security Verification Standard - Mobile Applikationen.
- OWASP Mobile Security Testing Guide.

Best Practices und Unterstützung werden jeweils durch die Security Advisor bereitgestellt, wie im Kapitel Methodology beschrieben.

2.4.2 Datenschutz

*Ansprechpartner*innen: Samantha Meindl, BWI; Fabian Angelstorf, BWI; Georg Hofmann, BWI*

Für den Themenkomplex Datenschutz gelten in der BWI vorrangig folgende Dokumente:

- Richtlinie Operativer Datenschutz.
- Verfahrensanweisung Aufbau einer Verarbeitungstätigkeit.
- Datenschutzkonzept Template (DSK Template).

Für die Softwareentwicklung sind insbesondere die folgenden Prinzipien umzusetzen:

- Das Prinzip "**Data Protection by Design**": Ziel ist es, bereits während des Designs von Systemen bzw. der Entwicklung das Thema Datenschutz zu berücksichtigen. Hierzu zählen Maßnahmen wie die Minimierung der Erhebung und Verarbeitung personenbezogener Daten, möglichst frühzeitige Pseudonymisierung bzw. (wenn möglich) Anonymisierung der Daten im Verarbeitungsprozess und die Beschränkung des Zugriffs auf die Daten durch Zugriffsstrukturen und -berechtigungen.
- Das Prinzip "**Data Protection by Default**": Hierbei ist darauf zu achten, dass im Auslieferungszustand die Grundeinstellungen im Sinne des Datenschutzes voreingestellt sind. Diese Einstellungen sollten von der nutzenden Person konfigurierbar sein. Zum Beispiel sollte festgelegt werden, welcher Umfang an personenbezogenen Daten bei Selektions-, Export- und Auswertungsfunktionen verfügbar bzw. vorausgewählt ist. Zudem ist darauf zu achten, die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben festzulegen (z. B. vorbefüllte Auswahlmöglichkeiten statt Freitextfelder).

Eine Übersicht über die Themen "Data Protection by Design" und "Data Protection by Default" ist der Guideline 4/2019 on Article 25 Data Protection by Design and by Default zu entnehmen. Weitergehende Anforderungen können zudem der ISO 31700 entnommen werden.

Die Umsetzung und die Einhaltung der Prinzipien wird im Anhang zum DSK Template "Fragebogen Privacy by Design und by Default" (siehe o. g. Datenschutzkonzept Template) nachgehalten.

- [MUSS]: Die im DSK Template aufgeführten Anforderungen (Fragebogen Privacy by Design und by Default, siehe Anhang) sind verpflichtend umzusetzen.
- [MUSS]: Das DSK Template ist gemeinsam für jedes Entwicklungsprojekt verpflichtend auszufüllen. Bei Bedarf kann hierfür die jeweilige Datenschutzfachkraft des Bereichs hinzugezogen werden (Kontakt: bwi.fp.datenschutzfachkraft@bwi.de).

3 Software Engineering Module

Das Software Engineering Module ist der wesentliche Kern des Software Engineering Frameworks. Das Modul beinhaltet die Standards zur Architektur, zum Design und zur Entwicklung von Software. Zudem werden Methoden zur Anforderungserhebung und Qualitätssicherung beschrieben.

3.1 Discovery & Validation

Ansprechpartner: Christoph Winkler, BWI

Eine Produktentwicklung basiert auf den Anforderungen, die an das Produkt gestellt werden. Die Entdeckung (Discovery) und Validierung (Validation) dieser Anforderungen, als essentielle Teile der Produktentwicklung, werden in diesem Kapitel erklärt.

3.1.1 Discovery

Definition

- Discovery ist die sprichwörtliche Entdeckungsarbeit am Produkt. Zu Anfang einer Produktentwicklung besteht die Discovery an der Erarbeitung und Befüllung des initialen Product Backlogs. Wichtig ist dabei, dass alle Anforderungen, die zum Projektstart bekannt sind, **zusammen mit dem Kunden** erhoben werden, um ein möglichst passendes Produkt für den Kunden zu entwickeln.
- Während der iterativen Produktentwicklung findet die Discovery kontinuierlich statt, indem Anforderungen fortlaufend mit dem Kunden zusammen besprochen und im Product Backlog dokumentiert werden. Dabei gehört nicht nur die Aufbereitung der initialen Anforderungen zur Discovery, sondern auch das "Entdecken" von neuen noch nicht erfassten Anforderungen.

Durchführung von Discovery

- Zur initialen Product-Backlog-Befüllung werden Methoden aus dem agilen Requirements Engineering verwendet. Agiles Requirements Engineering beschreibt dabei das Requirements Engineering unter Gesichtspunkten einer agilen Vorgehensweise (v.a. iterativ, kundenorientiert, dem Zeitpunkt entsprechend). Anforderungen an das Produkt werden hierbei zusammen mit dem späteren Umsetzungsteam und dem Kunden erhoben. Hieraus resultiert ein besseres Verständnis für die Anforderungen auf Seiten der Entwicklung und ein besseres technisches Verständnis auf Seiten des Kunden. Ebenfalls entfallen hierdurch zahlreiche Übergaben, bei denen Informationen zu den Anforderungen verloren gehen können. Die präferierte Methode ist das User Story Mapping von Jeff Patton. Es können ebenfalls andere agile Methoden für das Befüllen des Backlogs gewählt werden.
- Während der iterativen Produktentwicklung können weitere verschiedene agile Methoden für die "Entdeckung" von neuen Anforderungen genutzt werden wie z. B.:
  - Personas
  - Example Mapping oder
  - Impact Mapping.

3.1.2 Validation

Die Validation ist unterteilt in:

- **Produktvalidierung**
  - Alle Anforderungen, die an ein Produkt gestellt werden, sind in erster Linie Annahmen. Es wird also angenommen, mit Hilfe dieser Anforderungen das Problem des Kunden zu lösen bzw. das Bedürfnis des Kunden zu erfüllen. Daher muss noch vor dem Beginn der eigentlichen Entwicklung die initiale Validierung dieser Annahmen durchgeführt werden. Validierung bedeutet dabei, möglichst einfach und schnell Feedback z. B. durch die Nutzung von Prototypen zu sammeln, um festzustellen, ob die Annahmen richtig sind und man somit das richtige Produkt entwickelt.
  - In der laufenden Produktentwicklung müssen ebenfalls Validierungen von neuen Anforderungen durchgeführt werden.

- **Technische Validierung**
  - Die technische Validierung erfolgt fortlaufend und bezieht sich auf den programmierten Quellcode. Dieser wird technisch validiert. Dies geschieht mit Hilfe von automatisierten Tests (wie z. B. Unit-, Integration-, oder End2End Tests) oder manueller Validierung wie z. B. Prototyping.

Durchführung der Produktvalidierung

Analog zur Discovery kommen in der Validation ebenfalls agile Methoden zur Produktvalidierung zum Einsatz. Für die initiale Validierung des gesamten Produktes können Methoden wie das MVP oder der Lean Start Up Ansatz von Eric Ries genutzt werden. Grundlegend ist darauf zu achten, dass überhaupt eine Validierung der Anforderungen (bzw. Annahmen) **vor** der eigentlichen Produktentwicklung stattfindet. Hier gilt es die Validierung mit möglichst wenig Aufwand und geringen Mitteln umzusetzen.

Während der Produktentwicklung wird ebenfalls kontinuierlich das Produkt bzw. die Anforderungen validiert. Hierzu können Methoden wie z. B. das KANO Modell verwendet werden.

Durchführung der technischen Validierung

In Ergänzung zur generellen Produktvalidierung wird der programmierte Source Code kontinuierlich validiert. Hierfür bedient man sich an unterschiedlichen Hilfsmitteln:

- Automatisierte Validierung (siehe auch Kapitel Software Quality & Assurance)
  - Unit Tests
  - Integration Tests
  - End2End Tests
  - Performance Tests
  - Regressionstests
  - CI/ CD Pipeline

- Manuelle Validierung
  - Prototyping
  - Modeling (z. B. UML)
  - Pull Requests

3.2 Software Design

In diesem Kapitel werden Empfehlungen und Vorgaben für das Design einer Software - von der Architektur bis zum UX/UI-Design - aufgeführt. Zudem wird das Thema nachhaltige Softwareentwicklung behandelt.

3.2.1 Architecture & Design Engineering

Ansprechpartner: Arne Unruh, BWI; Florian Jost, BWI; Martin Becker, ZDigBw; Stephan Drews, ZDigBw

In agilen Projekten werden Architekturarbeiten sowie Softwaredesign gemeinsam mit den Features des Produktinkrements iterativ vom Projektteam weiterentwickelt. Den Rahmen für die Ausgestaltung bilden Vorgaben (Solution-Architektur, Richtlinien, usw.) und Projektziele (Qualität, Zeit, Kosten, Scope). Ein effizientes Design von komplexen Softwaresystemen zeichnet sich durch ein hohes Abstraktionsniveau aus und unterstützt somit die Wiederverwendung von Software.

Im Folgenden werden die Grundsätze, Methoden und Muster vorgestellt, die zur Erstellung einer Softwarearchitektur herangezogen werden können bzw. müssen (vgl. Kapitel Security & Compliance). Zudem sind die Vorgaben zur Dokumentationspflicht aufgeführt.

3.2.1.1 Grundsätze

Bei Architekturarbeiten sowie Softwaredesign ist folgendes zu beachten:

- [MUSS]: Bei der Erarbeitung des Designs und der Architektur einer Software müssen die Designansätze KISS, DRY und SOLID Anwendung finden. Die wesentlichen Aspekte leiten sich daraus ab:
  - Einfachheit - Das Konzept ist einfach zu halten (Erlernbarkeit, Umsetzbarkeit).
  - Wartbarkeit - Erhöhung der Wartbarkeit des Systems durch Isolierung funktionaler Verantwortlichkeiten.
  - Wiederverwendbarkeit - Wiederverwendbarkeit von Funktionen ermöglichen.
  - Einheitlichkeit - Das Konzept ist auf unterschiedliche Projekte anwendbar.
  - Nachvollziehbarkeit (Traceability) - Zuordenbarkeit der Anforderung zu den Artefakten und Verantwortlichkeiten.
  - Automatisierbarkeit - Maximierung der Automatisierung von Entwicklungs-, Test-, Integrations-, Release- und Konfigurationsprozessen.
  - Skalierbarkeit - Vertikale und horizontale Skalierbarkeit vorsehen.

3.2.1.2 Methoden

Folgende Methoden können bzw. müssen abhängig vom Entwicklungsvorhaben genutzt werden:

- [MUSS]: Es muss eine mehrschichtige Architektur implementiert werden.
  - [EMPFOHLEN]: Die Architektur ist in drei Hauptkategorien zu gliedern: Präsentation, Applikation und Infrastruktur.

- [MUSS]: Security by Default: Alle relevanten Sicherheitseinstellungen müssen als Grundeinstellung berücksichtigt werden (siehe auch BWI Architekturvorgabe AVIS04).

- [MUSS]: Security by Design: Das System soll robust und resilient gestaltet werden (gemäß CON.8.A22, siehe auch Orientierungshilfe Informationssicherheitsanforderungen im Anhang und BWI Architekturvorgabe AVIS03).
- [EMPFOHLEN]: Test Driven Development (TDD): Erstellung der Softwaretests vor der Programmierung zur Gewährleistung der Qualität und Lauffähigkeit.
- [EMPFOHLEN]: Software-as-a-Service Implementierung nach der Twelve-Factor App Methodology.
- [EMPFOHLEN]: Minimum Viable Product (MVP): Frühzeitige Bereitstellung eines minimal funktionsfähigen Produktes zum Einholen von Kundenfeedback und für iterative Erweiterungen (siehe Kapitel Discovery & Validation).
- [EMPFOHLEN]: Anti-Fragile: Berücksichtigung typischer Probleme, um diese von vorneherein einzuplanen und abfangen zu können, z. B. ein kurzzeitiger Ausfall einer Datenbank.
- [KANN]: Behaviour Driven Development (BDD) mit Domain Driven Design (DDD): Orientierung an der Fachlichkeit der Anwendungsdomäne zur Erleichterung der Kommunikation zwischen Entwickler*innen und Fachexpert*innen.

3.2.1.3 Muster

Abhängig vom Softwareprodukt müssen bzw. können folgende Muster bei der Erstellung der Architektur genutzt werden:

- [MUSS]: Verwendung von Standard-API-Technologien (Sicherstellung der Interoperabilität).
  - [EMPFOHLEN]: Nutzung von REST oder GraphQL.
- [MUSS]: Lose Kopplung von Komponenten und (Sub-) Systemen, Trennung durch Interfaces.
- [MUSS]: Softwarekomponenten müssen bei IP-basierter Kommunikation Hostnamen/DNS nutzen, da sich IP-Adressen zur Laufzeit ändern könnten.
- [MUSS]: Verwendung von Enterprise- und Design-Patterns.
- [MUSS]: Verwendung einer modularen Architektur, entweder Microservices oder modularer Monolith.
- [EMPFOHLEN]: Softwarekomponenten sollten möglichst stateless sein.
- [EMPFOHLEN]: Softwarekomponenten (und damit die gesamte Softwarearchitektur) sollten möglichst horizontal skalierbar und unabhängig von anderen Komponenten sein.
- [EMPFOHLEN]: Erreichung einer Zero-Down-Time während der Softwarebereitstellung (Blue-Green Deployment).
- [KANN]: Softwarekomponenten sollten Daten über standardisierte Schnittstellen, Message-Broker oder cloudfähige Datenbanken austauschen.
- [KANN]: Feature Toggling: Funktionalitäten aktivierbar oder deaktivierbar implementieren.

3.2.1.4 Dokumentationsvorgaben

Eine allgemeine Dokumentation ist gemäß CON.8.A12 verpflichtend. Dabei gilt:

- [MUSS]: Beschreibung des fachlichen und technischen Kontextes.
- [MUSS]: Dokumentation von Schnittstellen, inkl. Parameter, Ausnahmen, Beschreibung der Funktionalität.
- [MUSS]: Dokumentation von Architekturentscheidungen.
- [MUSS]: Dokumentation des Einsatzes von COTS / 3rd Party Software, inkl. Zweck der Verwendung.
- [MUSS]: Dokumentation der Fehlerfälle und -codes.
- [MUSS]: Dokumentation des Unternehmens gemäß Urheberrecht: Copyright © <Jahr> <Employer>
  - Beispiel: Copyright © 2024 BWI GmbH
  - Urheberrechte der extern eingebundenen Komponenten sind dokumentationsseitig zu beachten.
  - [KANN]: Erweiterung Urhebervermerk mit Autor: Copyright © <Jahr> <Employer>, <Author>
    - Beispiel: Copyright © 2024 BWI GmbH, Author John Doe
- [MUSS]: Zusätzliche Informationen wie beispielsweise Betriebs- und Nutzerhandbuch sind der Technischen Dokumentation hinzuzufügen.
- [EMPFOHLEN]: Verwendung der arc42 Templates.
- [EMPFOHLEN]: Modellierung von Systemen, Sub-Systemen und Komponenten inkl. deren Abhängigkeiten.
  - Modellierung im Kontext NATO bzw. Bw in NAF bzw. AdmBw.
  - Systemnahe Modellierung optimalerweise in UML.

3.2.1.5 Weiterführende Architekturrichtlinien

Die BWI ist an folgende Architekturrichtlinien gebunden, die auch in das Software Engineering Framework eingeflossen sind:

- Architekturrichtlinie für die IT des Bundes (Version 2022)
- BWI Architekturprinzipien (siehe Kapitel Architecture & Design Engineering)
- BWI Architekturvorgaben (siehe Kapitel Architecture & Design Engineering)

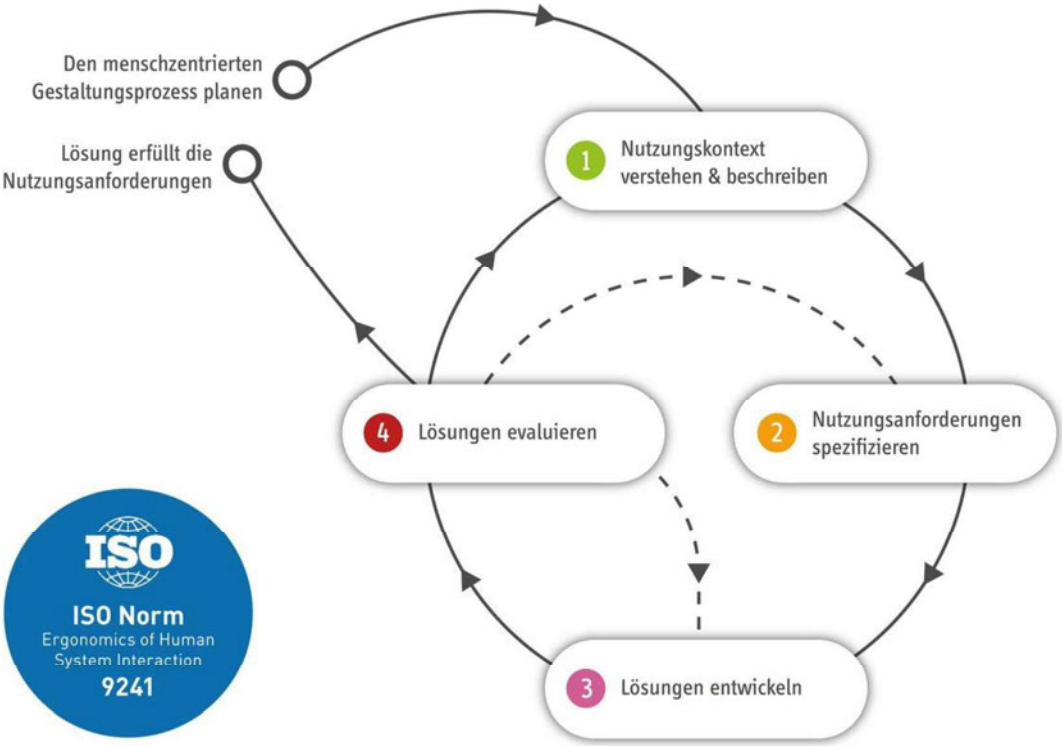
3.2.2 UX/UI Design

*Ansprechpartner*innen: Katrin Liebich, BWI; Dominik Röser, ZDigBw*

Einige grundlegende Definitionen zum Thema UX/UI Design sind im Glossar abgelegt.

3.2.2.1 UX/UI Prozess

Der menschzentrierte Gestaltungsprozess ist Teil der Normenfamilie ISO 9241 und umfasst folgende Schritte:



Quelle: Human centered design nach DIN ISO 9241: rocket-media

Planung

- [MUSS]: Generell iterative Entwicklung berücksichtigen (Lean UX).
- [EMPFOHLEN]: Ziel definieren (angestrebtes Arbeitsergebnis).
- [EMPFOHLEN]: Interessenvertreter definieren.
- [KANN]: UX Plan erstellen.

Phase 1: Analyse des Nutzungskontextes (verstehen und spezifizieren)

- [MUSS]: Benutzertypen analysieren (primär, sekundär, indirekt).
- [MUSS]: Benutzerziele definieren (grundsätzliches Bedürfnis des Benutzers in realen Welt).
- [EMPFOHLEN]: Aufgaben evaluieren (+ Teilaufgaben).
- [EMPFOHLEN]: Ressourcen analysieren (Ausrüstung, Informationen, Unterstützung, Zeit, menschliche Anstrengung, finanzielle Ressourcen, Materialien).
- [EMPFOHLEN]: Umgebung analysieren (physische, soziale, technische Bedingungen).
- [EMPFOHLEN]: Herausforderungen/ Probleme spezifizieren.
- [KANN]: Methoden anwenden (z. B. kontextuelles Interview, (Online-) Umfrage, Feldbeobachtung, Fokusgruppe, Tagebuchstudie).
- [KANN]: Nutzungskontextbeschreibung erstellen in Form von:
  - Benutzer: Benutzergruppenprofile, Personas.
  - Ziele: Ist-Szenarien.
  - Aufgaben: Aufgabenmodelle, Ist-Szenarien, User Journey Maps.
  - Ressourcen: Ist-Szenarien.
  - Umgebung: Listen, Ist-Szenarien.

Phase 2: Spezifizieren der Nutzungsanforderungen

- [MUSS]: Erfordernisse der Benutzer ableiten.
- [MUSS]: Konkrete Nutzungsanforderungen an das interaktive System (IS) ableiten.
  - Qualitative + quantitative Nutzungsanforderungen berücksichtigen.
  - Marktanforderungen (Vorgaben des Unternehmen, z. B. Absatzsteigerung, Zielgruppenänderung, Style Guide Vorgaben) und organisatorische Anforderungen (gesetzliche Anforderungen, z. B. AGB) berücksichtigen.

Phase 3: Erzeugen von Gestaltungslösungen

- [MUSS]: Identifizierte Nutzungsanforderungen in ein funktionierendes IS überführen, möglich über folgende Schritte (mit regelmäßigen Feedbackschleifen über den Nutzer):
  - [KANN]: Frühes Design erzeugen.
    - [KANN]: Darstellung in Form von:
      - Nutzungsszenarien (textuelle Beschreibung).
      - Storyboards.
      - User Journey Maps.

- [EMPFOHLEN]: Erste Entwürfe erzeugen.
  - [EMPFOHLEN]: Informationsarchitektur erstellen.
    - [KANN]: Anwendung von Methoden (z. B. „Card Sorting“).
  - [EMPFOHLEN]: Navigationsstruktur erstellen.
  - [EMPFOHLEN]: Feedback einholen.
  - [KANN]: Wireframes erstellen (analog oder digital).
  - [KANN]: Low Fidelity-Prototyp erstellen (analog oder digital).
- [EMPFOHLEN]: High-Fidelity-Prototyp erzeugen.
  - [EMPFOHLEN]: Ähnelt dem fertigen IS.
  - [EMPFOHLEN]: Feedback einholen / frühzeitige Usability Evaluierung ermöglichen.
  - [EMPFOHLEN]: Richtlinien für Usability berücksichtigen:
    - Richtlinien der BITV Version 2.0 zur Barrierefreiheit.
    - 7 Dialogprinzipien (Normreihe ISO 9241): Aufgabenangemessenheit, Selbstbeschreibungsfähigkeit, Erwartungskonformität, Lernförderlichkeit, Steuerbarkeit, Individualisierbarkeit, Fehlertoleranz.
    - Benutzerunterstützung.
    - Heuristiken.
    - Projektspezifische Gestaltungsregeln (Style Guide).
  - [EMPFOHLEN]: Visuelles Design mit einbeziehen.
  - [EMPFOHLEN]: Design System anlegen.

Phase 4: Evaluieren des Designs (gegen Nutzungsanforderungen)

- [EMPFOHLEN] in Form von:
  - Usability-Test (unmoderierter/ moderierter (Remote-) Test).
  - Benutzerbefragung.
  - Usability-Inspektion.

Durch die Evaluierung werden einerseits neue Informationen über die Bedürfnisse der Benutzer und andererseits über die Stärken und Schwächen der Gestaltungslösung gesammelt. Diese Ergebnisse fließen dementsprechend wieder in Phase zwei oder drei ein, so dass ein iterativer Prozess entsteht. Sollten keine Optimierungen mehr notwendig sein, ist eine Folge-Evaluierung in regelmäßigen Abständen (z. B. einmal im Jahr oder bei beeinflussenden Veränderungen auch schon früher) empfehlenswert.

Generell müssen diese vier Phasen nicht als linearer Prozess bearbeitet werden. Wie die Grafik oben verdeutlicht, kann zu derjenigen Phase gesprungen werden, die für die momentane Entwicklungsphase am sinnvollsten ist. Meist ist es aber sinnvoll, mit einem Analyseschritt zu starten. Sei es, um den Nutzungskontext zu verstehen oder beispielsweise um die Ergebnisse eines Usability-Tests zu interpretieren.

Wichtig ist, dass der Benutzer und andere Stakeholder bereits in einer frühen Phase mit in den Prozess einbezogen werden und dass dieser iterativ abläuft. Denn viele Bedürfnisse und Erwartungen zeichnen sich erst im Laufe der Entwicklung, aufgrund stetigem Erkenntnisgewinns ab.

3.2.3 Sustainable Programming

Ansprechpartnerinnen: Janina Moser, BWI; Samantha Meindl, BWI

In der Nachhaltigkeitsforschung wird zwischen vier verschiedenen Formen der Nachhaltigkeit unterschieden: ökologisch, technisch, sozial und ökonomisch. Dieses Kapitel beschäftigt sich mit der ökologischen Dimension der Nachhaltigkeit: Software wird auf Hardware ausgeführt und verursacht CO2-Emissionen durch den Energieverbrauch und den Erneuerungszyklus. Das Ziel der ökologischen Dimension der Nachhaltigkeit ist daher Emissionen von Software so weit wie möglich zu minimieren.

Die Herausforderung in der nachhaltigen Software-Entwicklung besteht darin, kontinuierlich nicht nur die direkten Emissionen, sondern auch indirekte Scope 3 Emissionen zu berücksichtigen, die z. B. durch die eigentliche Nutzung der Software entstehen werden:

- Die Nutzer*innen der Software haben während der Nutzung nur wenig Einfluss auf die Effizienz der Software. Den Einfluss haben hauptsächlich die Softwareentwickler*innen während der Entwicklung.
- Die positive Auswirkung einer Codeoptimierung hinsichtlich der Effizienz einer Software ist bei einer vielfach genutzten Software umso größer und hat mehr Einfluss als ein effizientes Nutzungsverhalten einzelner Nutzer*innen.

[MUSS]: Verpflichtende Aktivitäten

- Bewusstsein für Nachhaltigkeit im Team und bei allen relevanten Stakeholdern bereits zu Beginn des neuen Software-Engineering-Vorhabens schaffen.
- Verhaltensweisen zur Gewohnheit machen wie:
  - Trennen des Computers vom Strom bei Nichtbenutzung.
  - Ungenutzte Ressourcen (VMs, Anwendungen, Services…) schließen.

[EMPFOHLEN]: Optionale Aktivitäten

- Abhängig von den Anforderungen an ein neues Software-Engineering-Vorhaben bei der Auswahl von Programmiersprachen und Frameworks auch die Energieeffizienz (soweit bekannt) berücksichtigen: Es existieren beispielsweise Sprachen-Benchmarks hinsichtlich Energie, Zeit- und Speichereffizienz. Jedoch ist keine einzelne Sprache in allen Kriterien die beste.
- Häufig verwendete Features mit höherem Stromverbrauch identifizieren, insbesondere in der Innermost Loop, welche Anteile der Software werden am meisten genutzt oder haben den höchsten Verbrauchswert?
- Es existieren verschiedene Methoden, um den Stromverbrauch (abhängig von der Art der Software) zu berechnen. Eine Liste von Tools ist hier zu finden: GitHub - Green-Software-Foundation/awesome-green-software
  Beispiele sind:
  - jPowerMonitor: Messungen des Energieverbrauchs auf Unit-Test bzw. Methoden-Ebene für Java-Prozesse.
  - Website Carbon Calculator: Ein CO2–Rechner für Webseiten.
  - Intel RAPL (Running Average Power Limit): Messung der CPU-Nutzung.
  - PowerAPI: Software Suite, die den Verbrauch auf Device-, Prozess- und Anwendungsebene messen kann.
  - DockerCap: für Power Budgeting auf Container-Ebene.

- Wenn möglich, Datennutzung reduzieren durch beispielsweise:
  - Effizientes Caching: Identifikation der zu cachenden Daten durch Klassifizierung der Daten nach Nutzungsdauer; naher Cache an den Nutzer*innen und Caching auf verschiedenen Leveln berücksichtigen.
  - Minimierung des Datenaustauschs in die Cloud durch beispielsweise komprimieren/dekomprimieren, aggregieren der Daten mittels Edge und Fog Computing.
  - Kleinere Größen für Bilder und andere Medien.
  - Progressive Web Applications in Betracht ziehen, da durch das Caching nach dem initialen Laden die Ladezeit aber auch Emissionen reduziert werden.
  - Sparsamer Einsatz von Externen Abhängigkeiten: Externe Abhängigkeiten nur dort verwenden, wo sie wirklich benötigt werden (Bsp.: Nutzung kleiner Images als Docker Basis Images; Eigene Implementierungen statt Nutzung externer Bibliotheken, falls die Anforderungen einfach/minimal genug sind).
  - Datenkomprimierung und Begrenzung der Datenübertragung (z. B. GraphQL für REST-APIs nutzen).
  - Verwendung effizienter Algorithmen und Datenstrukturen (Big-O).
  - Minimieren der Speichernutzung.
  - Anwendung modularer und wiederverwendbarer Entwurfsmuster (z. B. Microservices), um die Skalierbarkeit zu erhöhen.
  - Regelmäßiges Testen und Debuggen des Codes.
  - Klare und konsistente Dokumentation des Codes.

- In bestehender Software
  - ungenutzte Funktionen entfernen oder überarbeiten, auch in externen Komponenten beispielsweise durch Tree-Shaking bei der Nutzung von JavaScript.
  - Endlosschleifen überarbeiten, die unnötige Energie verbrauchen, wie Polling eines nicht erreichbaren Servers.

- Maßnahmen zur Optimierung einer Microservices Architektur: Principles.Green.

Hinweis: Diese Maßnahmen bieten erste Möglichkeiten, CO2-Emissionen von Software zu reduzieren. Sie erheben keinen Anspruch auf Vollständigkeit und werden im Rahmen weiterer Software Engineering Framework Releases aktualisiert und weiter vervollständigt.

Die Berücksichtigung des Energieverbrauchs kann nur unter Abwägung aller funktionalen und auch nicht-funktionalen Anforderungen wie Sicherheit und Verfügbarkeit gewährleistet werden.

Weiterführende Links

- https://greensoftware.foundation/articles/10-recommendations-for-green-software-development
- https://www.gft.com/cn/en/technology/thought-leadership
- Kurs Sustainable Software Engineering: https://open.hpi.de/courses/sustainablesoftware2022/overview
- https://www.iese.fraunhofer.de/blog/sustainable-software-design/

3.3 Coding Guidelines

*Ansprechpartner*innen: Frank Rotermund, BWI; Koidu Spiess, BWI; Markus Kobler, BWI; Rico Giacu, ZDigBw*

Dieses Kapitel enthält allgemeine und programmiersprachenspezifische Richtlinien. Es steht im Einklang mit den Architekturprinzipien der BWI: AP04 Beherrschbarkeit, AP07 Erweiterbarkeit, AP09 Robustheit, AP12 Skalierbarkeit und AP13 Standardisierung.

Die Nutzung einer einheitlichen Coding Guideline bietet folgende Vorteile:

- Synergiepotenzial und hohe Entwicklungsleistung durch eine homogene Vorgehensweise.
- hohe Qualität der Software durch standardisierte
  - Lesbarkeit,
  - Wartbarkeit,
  - Robustheit bei Änderungen,
  - Testbarkeit und
  - Sicherheit.

Die vorliegende Coding Guideline ist nicht BWI-individuell, sondern hält sich mit wenigen Ausnahmen an die etablierte Arbeitsweise der globalen Communities.
Vorteile der Anwendung etablierter Guidelines sind:

- neue Mitarbeiter aus Wissenschaft und Industrie müssen nicht umgelernt werden.
- Grundsatzdiskussionen werden vermieden.
- Es entstehen keine Aufwände durch Pflege einer von Grund auf eigenen Guideline.

Die Coding Guideline besteht aus einer Allgemeinen Guideline und aus programmiersprachenspezifischen Guidelines, die in den folgenden Kapiteln beschrieben werden.

3.3.1 Allgemeine Guideline

*Ansprechpartner*innen: Frank Rotermund, BWI; Koidu Spiess, BWI; Markus Kobler, BWI; Rico Giacu ZDigBw*

Dieses Kapitel fasst die generischen Richtlinien zusammen, die gleichermaßen für alle im Software Engineering Framework erfassten Programmiersprachen gelten. Von den aufgeführten Anforderungen ist folgender Code ausgenommen:

- Source Code aus einem Code Generator.
- Source Code aus externen Quellen, der nicht von einem Anbieter der BWI oder Bw stammt (z. B. aus einer Open Source Community).
- Legacy Code, der nicht mehr weiterentwickelt oder nur noch minimal verändert wird.

Guidelines

- [MUSS]: Sprachspezifische Guidelines, die nicht durch das Software Engineering Framework abgedeckt werden, sind in der Projektdokumentation festzuhalten.
- [MUSS]: Jedes Softwareprojekt referenziert in seiner Projektdokumentation die jeweils verwendete Version des Software Engineering Frameworks.
- [MUSS]: Grundsätzlich sind bei der Programmierung die Clean Code Best Practices nach Robert C. Martin anzuwenden [Mar08].

Sprachkonventionen

- [EMPFOHLEN]: Quellcode inklusive Kommentierung ist auf Englisch zu schreiben.
- [EMPFOHLEN]: Das Änderungsprotokoll sowie die README-Datei und ggf. weitere Dateien sind auf Englisch zu schreiben.

API-Dokumentation

- [MUSS]: Eine Dokumentation der öffentlichen Anteile der API ist gemäß CON.8.A12 zu verfassen.
- [KANN]: Die Entscheidung, ob private Funktionen eine API-Dokumentation erhalten, obliegt dem Projekt.

Inline-Dokumentation

- [MUSS]: Code muss so weit wie möglich selbsterklärend sein.
- [EMPFOHLEN]: Für notwendige Erklärungen sollten Inline-Kommentare verwendet werden.

README-Datei

- [MUSS]: Jedes Code-Projekt muss eine README-Datei auf oberster Ebene im Quellcodeverzeichnis pflegen. Dies garantiert die Auffindbarkeit der Datei.
- [MUSS]: Die README-Datei enthält folgende Informationen: (Template für README im Anhang)
  - Zweck der Software.
  - Link zum Repository des Versionskontrollsystems.
  - Link zum Projekt im CI/CD-Tool.
  - Link zum Projekt im Issue-Tracking-System.
  - Link zur weiterführenden Dokumentation des Projekts.
  - Kurzanleitung zum Starten der Software.

    - Rein namentliche Auflistung anderer zum Betrieb der Software notwendigen Systeme.

- [EMPFOHLEN]: Optional enthält die README-Datei bei Backendprojekten:
    - Konfigurationsmöglichkeiten der Software.
    - Kurzanleitung zum Deployment der Software.

Lizenzierung

- [MUSS]: Jedes Code-Projekt muss eine LICENSE-Datei auf oberster Ebene im Quellcodeverzeichnis pflegen.
- [MUSS]: Die LICENSE-Datei enthält die Lizenz unter der das Projekt veröffentlicht wird.

Versionierung

- [MUSS]: Einzelne Versionen einer Software werden über Versionsnummern identifiziert, entsprechend der semantischen Versionierung.
    - Dieses System ist nach dem Schema *MAJOR.MINOR.PATCH* aufgebaut:
        - *MAJOR* sollte erhöht werden, wenn sich die API ändert, z. B. weil die Software eine große neue Funktion, ein Redesign oder eine andere große Änderung erhalten hat.
        - *MINOR* sollte erhöht werden, wenn Funktionalitäten verändert werden, die Änderungen aber abwärtskompatibel sind.
        - *PATCH* sollte bei einer abwärtskompatiblen Bugfixes erhöht werden.

Änderungsprotokoll / Release Notes

- [MUSS]: Mit jeder Software wird ein Änderungsprotokoll ausgeliefert.
- [MUSS]: Das Änderungsprotokoll besitzt das folgende Minimalformat:

```
Release 0.1.1

Breaking Changes

   <description>

Bugfixes
    [ABC-2350] - <description>

Improvements
    [ABC-4943] - <description>
```

- [MUSS]: In der BWI gelten des Weiteren die BWI-Anforderungen der Informationssicherheit (Vorgabe DEV.A3) für Release Notes. Daraus ergibt sich folgender weiterer Inhalt:
    - Umfang der erhobenen Protokolldaten (Tracking).
- [MUSS]: Das Änderungsprotokoll wird mit jedem Release nachgezogen, indem das aktuelle Release am Anfang der Datei eingefügt wird.

- [MUSS]: Jeder Bugfix und jede Weiterentwicklung haben jeweils eine eindeutige Kennung, mit deren Hilfe sie im Ticketverwaltungssystem nachgeschlagen werden können.
- [EMPFOHLEN]: Release Notes können darüber hinaus Folgendes beinhalten:
  - Korrekturdatum.
  - Baseline, auf die sich die Korrektur bezieht.
  - Betriebssystem laufende Version.
  - Umgebungsvariablen / Informationen zum Konfigurationsmanagement.
  - Entwickler*in, der/die die Korrektur durchgeführt hat.

Toolgestützte Prüfung der Guideline während der Entwicklung

- [EMPFOHLEN]: Die IDE soll soweit möglich die Einhaltung der Guideline automatisch überprüfen. Entweder sind die Guideline-Regeln in die IDE fest integriert oder es wird eine Style-Datei in die IDE eingelesen.

Toolgestützte Prüfung der Guideline in der CI-Pipeline

- [MUSS]: SonarQube muss mindestens mit default Quality Profile in die CI-Pipeline eingebunden sein. Dadurch ergeben sich weitere Coding Regeln aus SonarQube .
- [EMPFOHLEN]: Je nach Projektanforderungen ist es ratsam, in SonarQube einen eigenen Quality Profile vom default Quality Profile abzuzweigen.
- [EMPFOHLEN]: Je nach Projektanforderungen ist es ratsam, in SonarQube einen eigenen Quality Gate vom default Quality Gate abzuzweigen.
- [EMPFOHLEN]: Je nach Projektanforderungen ist es ratsam, Vulnerability Scans über den Code bzw. über die genutzten Drittbibliotheken durchzuführen.

Entwicklungsumgebung

- [MUSS]: In der Projektdokumentation muss die zu verwendende(n) IDE(s) festgehalten werden.
- [EMPFOHLEN]: Es sollte die aktuelle, mit dem Code kompatible, stabile Version verwendet werden.
- [EMPFOHLEN] Innerhalb eines Teams sollte die gleiche IDE verwendet werden, um Konfigurationsprobleme zu minimieren.

Logging

- [EMPFOHLEN]: Verwendung folgender Log-Level:
  - DEBUG
    Informationen für die Diagnose von Problemen und die Fehlerbehebung.
  - INFO
    Wichtige Information um die Arbeitsweise der Anwendung nachzuvollziehen oder zu dokumentieren.
  - WARN
    Fehler, der zu keiner Ausnahme führt, kann behoben werden.
  - ERROR
    Fehler, der zu einer Ausnahme führt, muss behoben werden.
  - FATAL
    Fehler, der die ganze Anwendung beeinflusst, muss schnellstmöglich behoben werden.

- [EMPFOHLEN]: Möglichkeit zur Filterung von Logging Informationen für verschiedene Anforderungen (z. B. unter Datenschutzaspekten).
- [EMPFOHLEN]: Structured Logging für die Level DEBUG, INFO und WARN im JSON Format mit mindestens folgendem Inhalt:
  - Zeitpunkt des Eintrags (YYYY-MM-DD hh:mm:ss.SSS)
  - Log-Level
  - Sprechende Beschreibung
- [EMPFOHLEN]: Structured Logging für die Level ERROR und FATAL im JSON Format mit mindestens folgendem Inhalt:
  - Zeitpunkt des Eintrags (YYYY-MM-DD hh:mm:ss.SSS)
  - Log-Level
  - Fehlercode
  - Sprechende Beschreibung
  - Stack-Trace

Lokalisierung

- [MUSS]: Bei mehrsprachigen Applikationen müssen die Texte für die Lokalisierung an einer zentralen Stelle auffindbar sein.

3.3.2 C#

Ansprechpartner: Markus Kobler, BWI; Rico Giacu, ZDigBw, Stephan Drews, ZDigBw

Diese Coding Guideline dient gemeinsam mit der allgemeinen Guideline als Leitfaden für die Entwicklung mit der Programmiersprache C#.

Coding Guideline Grundlagen

Die folgenden Referenzen bilden maßgeblich die stilistischen Konventionen für die Entwicklung von C#-Code:

- Basis C# Style Guide von Microsoft.
- Dotnet Runtime Style Guide zur Erweiterung und Ergänzung des C# Basis Style Guides.
- C#-Code Formatierung in Visual Studio.

IDE

- [EMPFOHLEN]: Als Entwicklungsumgebung kann Rider von JetBrains eingesetzt werden.
- [KANN]: Als Entwicklungsumgebung kann auch Microsoft Visual Studio verwendet werden.
  - [MUSS]: Wird Microsoft Visual Studio als IDE verwendet, ist der Einsatz der Erweiterung ReSharper von JetBrains verpflichtend.

Formatierung

- [EMPFOHLEN]: Bei Bestandsprojekten sollte die vorhandene Formatierung übernommen werden.
- [EMPFOHLEN]: Die Default EditorConfig von Microsoft für C# wird verwendet.

3.3.3 C++

Ansprechpartner: Markus Kobler, BWI

Diese Coding Guideline dient gemeinsam mit der allgemeinen Guideline als Leitfaden für die Entwicklung mit der Programmiersprache C++.

Coding Guideline Grundlagen

Die folgenden Referenzen bilden maßgeblich die stilistischen Konventionen für die Entwicklung von C++-Code:

- C++ Core Guidelines von Bjarne Stroustrup und Herb Sutter.

IDE

- [EMPFOHLEN]: Als Entwicklungsumgebung kann Rider von JetBrains eingesetzt werden.
- [KANN]: Als Entwicklungsumgebung kann auch Microsoft Visual Studio verwendet werden.
  - [MUSS]: Wird Microsoft Visual Studio als IDE verwendet, ist der Einsatz der Erweiterung ReSharper von JetBrains verpflichtend.

Formatierung

- [EMPFOHLEN]: Bei Bestandsprojekten sollte die vorhandene Formatierung übernommen werden.
- [EMPFOHLEN]: Formatierungsregeln werden generell im Projekt festgelegt. Je nach Umgebung sollte der clangformat oder EditorConfig-Standard verwendet werden.
- [EMPFOHLEN]: Die von Visual Studio unterstützten EditorConfig Settings sind hier beschrieben.

Testing Frameworks

- [EMPFOHLEN]: Als Testing Framework wird googletest verwendet.

3.3.4 Java

Ansprechpartner: Felix Lambertz, BWI; Koidu Spiess, BWI

Diese Coding Guideline dient gemeinsam mit der allgemeinen Guideline als Leitfaden für die Entwicklung mit der Programmiersprache Java.

Coding Guide Grundlagen

- [MUSS]: Anwendung des Google Java Style Guides.
- [EMPFOHLEN]: Einhaltung der nachfolgend beschriebenen Abweichungen zum Style Guide:

Nr.	Kapitel	Titel	Abweichung
1	3.4.2	Ordering of class contents	High-level-Funktionen sollen zuerst in einer Klasse definiert sein, aufgerufene Funktionen sind weiter unten zu finden. Die aufgerufenen Funktionen dürfen dabei direkt nach der aufrufenden Funktion kommen.
2	4.8.5	Annotations	Die Ausnahmen für Annotations, die es erlauben, dass diese auf der gleichen Zeile wie der annotierte Code stehen, sind gestrichen. Annotations müssen immer in den Zeilen vor dem annotierten Code stehen. Für Parameter-bezogene Annotationen gilt dies nicht, diese können auch inline verwendet werden.
3	5.2.8	Type variable names	Die zweite Anforderung („A name in the form used for classes […]“) aus dem Style Guide wird gestrichen und gilt nicht.
4	7.3	Where Javadoc is used	JavaDoc ist nicht verpflichtend bei protected members. Public members von Klassen mit der Sichtbarkeit package sollten dagegen mit JavaDoc versehen sein.

- [EMPFOHLEN]: Anwendung der Richtlinien aus Secure Coding Guidelines for Java SE.

IDE

- [EMPFOHLEN]: IntelliJ
  - [EMPFOHLEN]: Einbindung der Google Java Style Guide Datei für IntelliJ.
- [KANN]: Eclipse
  - [EMPFOHLEN]: Einbindung der Google Java Style Guide Datei für Eclipse.

Testing

- [KANN]: JUnit mit Mockito.
- [KANN]: Spock-Framework.

EditorConfig

- [KANN]: Nutzung der .editorconfig (im Anhang) - Die Datei wurde auf Basis der Google Java Style Guide Datei für IntelliJ erstellt.

3.3.5 JavaScript und TypeScript

Ansprechpartner: David Reypka, BWI; Dany Meyrose, ZDigBw

Diese Coding Guideline dient gemeinsam mit der allgemeinen Guideline als Leitfaden für die Entwicklung mit den Programmiersprachen JavaScript und TypeScript.
Der Fokus liegt hierbei in der Web-Frontend-Entwicklung.

Coding Guide Grundlagen

- [MUSS]: Ein einheitlicher ESLint Regelsatz, der für alle Javascript Repos im Projekt definiert wird, muss erstellt werden. Die Kriterien dafür sind dem Absatz ESLint zu entnehmen, kann aber nach eigenem Ermessen erweitert werden.
- [MUSS]: Die Richtlinien des Clean Codes angepasst an JavaScript und TypeScript müssen beachtet werden.

IDE

- [EMPFOHLEN]: VS Code mit den Plugins Editorconfig, ESLint und Prettier.
- {Lizenzpflichtig} [EMPFOHLEN] JetBrains WebStorm oder JetBrains IntelliJ.

Dependency Management / Building

- [MUSS]: Nutzung der projektspezifischen package.json.
- [EMPFOHLEN]: Nutzung von entweder npm, pnpm oder yarn als package manager und nicht gemischt (Für Abhängigkeiten zwischen mehreren Projekten wird yarn mit workspaces empfohlen).
- [EMPFOHLEN]: Vite als Build Tool um Projekt zu erstellen und zu bundeln.
- {ANGULAR} [EMPFOHLEN]: Angular CLI als Command-Line Interface und Building Tool.

TypeScript

- [MUSS]: Verwendung von Typescript als Precompiler in allen Javascript Projekten.
- [MUSS]: Eine konsequente Typisierung von Variablen und Funktionen mittels TypeScript ist verpflichtend.
- [EMPFOHLEN]: Typescript im strict mode nutzen.

Frontend Frameworks

- [EMPFOHLEN]: React ist das bevorzugte Framework zur Entwicklung von WebFrontends.
- [KANN]: Angular, Vue, und Vanilla JavaScript (+evtl. JQuery) sind zulässig, wenn die Entscheidung auf einer fundierten Architekturentscheidung beruht.

Styling / UI Library

- [EMPFOHLEN]: Nutzung eines CSS-Präprozessors wie SCSS oder SASS.
- [EMPFOHLEN]: Nutzung einer Style/Component Library auf Basis von Tailwind.
- [KANN]: Bootstrap, Material Design und Prime (React, Vue, Angular) als alternative Style/Component Library.

Testing

- [EMPFOHLEN]: Vitest ist als Testrunner zu empfehlen.
- [KANN]: Jest als Testrunner.
- [EMPFOHLEN]: Cypress, Playwright oder TestCafé als E2E Test Framework, falls keine anderweitige Lösung oder dedizierte Tester*in.
- {ANGULAR} [EMPFOHLEN] Karma Jasmine als Testrunner.
- {ANGULAR} [EMPFOHLEN]: Component Harness ist zum Testen insbesondere von Angular Material Komponenten zu verwenden.

Scaffolding

- {REACT}[EMPFOHLEN] Zur Projekterstellung BWI React Starter nutzen oder vite-create --template react-ts nutzen.
- {VUE}[EMPFOHLEN] Zur Projekterstellung vite-create --template vue-ts.

Dokumentation

- {ANGULAR} [EMPFOHLEN]: (Entwickler-)Dokumentation der Software mit compodoc.

Internationalisierung

- {ANGULAR} [KANN]: Angular Internationalization (i18n) als Internationalisierung/Übersetzungswerkzeug.

Style Guide Anwendung

Für React wurde der Guide im BWI React Starter Projekt umgesetzt.

Tools

Folgende Developer Libraries unterstützen die Anwendung des Guides im Projekt:

- [MUSS]: ESLint - Statische Codeanalyse.
- [MUSS]: Prettier - Code Formatierung.
- [EMPFOHLEN]: Editorconfig - OS- und plattformübergreifende Workspace Parameter.
- [EMPFOHLEN]: Stylelint - Formatierung von Stylesheets.
- [EMPFOHLEN]: HTMLLint - Formatierung von HTML Dokumenten.
- [EMPFOHLEN]: Husky - PreCommit Hooks zur Codeprüfung vor dem Commit ins Repo.

Eslint Regeln

Folgende Konfigurationen können bzw. müssen für ESLint angewendet werden:

- [MUSS]: eslint:recommended (Basisregelsatz)
- [MUSS]: TypeScript-ESLint (Basisregelsatz Typescript)
- [EMPFOHLEN]: eslint-plugin-editorconfig (Abgleich mit Editorconfig Regeln)
- [EMPFOHLEN]: jsx-a11y (Barrierefreiheitsprüfung)
- [EMPFOHLEN]: sonarjs/recommended (Sonarqube Vorprüfung)
- [EMPFOHLEN]: eslint-plugin-unicorn.
- [EMPFOHLEN]: eslint-plugin-prettier.

- [EMPFOHLEN]: eslint-plugin-import
- {REACT} [EMPFOHLEN]: eslint-plugin-react/recommended
- {REACT} [EMPFOHLEN]: eslint-plugin-react/jsx-runtime
- {REACT} [EMPFOHLEN]: eslint-plugin-react-hooks
- {VUE} [EMPFOHLEN]: eslint-plugin-vue
- {ANGULAR} [EMPFOHLEN]: Angular-ESLint

EditorConfig (im Anhang)

```
# EditorConfig file
root =  true
[*]
end_of_line = lf
insert_final_newline =  true
indent_size =  2
charset = utf-8
indent_style = space
max_line_length =  120
trim_trailing_whitespace =  true
```

3.3.6 Kotlin

Ansprechpartner: Georg Hofmann, BWI; Fabian Witte, ZDigBw

Diese Coding Guideline dient gemeinsam mit der allgemeinen Guideline als Leitfaden für die Entwicklung mit der Programmiersprache Kotlin.

Coding Guide Grundlage

- [MUSS]: Als generelle Basis an Richtlinien werden die Kotlin Coding Conventions festgelegt.
- [MUSS]: Die Prüfung der Kotlin Coding Conventions muss in der IDE aktiviert werden.
- [EMPFOHLEN]: Ktlint wird als Tool zur Prüfung der Kotlin Coding Conventions in der Pipeline empfohlen.

IDE

Android Projekte

- [MUSS]: Bei Android Projekten muss Android Studio als IDE verwendet werden.
- [EMPFOHLEN]: Es sollte nach Möglichkeit immer die aktuelle stabile Version von Android Studio genutzt werden.

Andere Projekte

- [EMPFOHLEN]: Als IDE für Kotlin ist IntelliJ zu empfehlen.

Testing

- [EMPFOHLEN]: JUnit für Unit Tests.
- [EMPFOHLEN]: mockk zum Mocken von Abhängigkeiten.

3.3.7 Python

Ansprechpartner: Jan Strohschein, BWI; Fabian Köhlinger, BWI

Diese Coding Guideline dient gemeinsam mit der allgemeinen Guideline als Leitfaden für die Entwicklung mit der Programmiersprache Python.

Coding Guide Grundlagen

- [MUSS]: Als generelle Basis an Richtlinien wird PEP8 festgelegt.
- [MUSS]: Es werden die auf Python angepassten Clean Code Prinzipien nach "Robert C. Martin" sinnvoll angewendet.

IDE

- [EMPFOHLEN]: VS Code mit den Plugins ms-python.python
- [EMPFOHLEN]: Package Manager für Data Science (z. B. Anaconda oder Mamba) zur Nutzung von Jupyter, TensorFlow, etc.
- [KANN]: JetBrains PyCharm.

Dependencies/Packaging

- [EMPFOHLEN]: Dependencies werden komplett über Poetry verwaltet.
  - [EMPFOHLEN]: `poetry install` generiert komplette Dependency Resolution in `poetry.lock`.
  - [EMPFOHLEN]: `poetry build` generiert `sdist` und `wheel`.
  - [EMPFOHLEN]: `poetry publish` veröffentlicht die Pakete im geeigneten Binärartefakt Repo (z. B. auch Nexus).

- [KANN]: Pip als Alternative zu Poetry kann benutzt werden.
  - [KANN]: Nutzung der projektspezifischen requirements.txt.
  - [KANN]: Konfiguration einzelner Tools und des Build-Systems kann in der `pyproject.toml` Datei vorgenommen werden.
  - [KANN]: Zum Paketieren kann `wheel` verwendet werden, beispielsweise mit: `python setup.py sdist bdist_wheel`
  - [KANN]: Wenn nötig, können weitere projektspezifische Felder in der `setup.py` gesetzt werden.
  - [KANN]: Wenn ein Upload zu einem PyPi-Repository vorgesehen ist, kann `twine` verwendet werden, beispielsweise mit: `twine upload --repository testpypi dist/*`

Virtual Environment

- [EMPFOHLEN]: Verwendung der von Poetry angelegten virtuellen Environments für die Projekte.
- [KANN]: Alternativ kann für die Erstellung eines Virtual Environment das Python Modul `venv` verwendet werden: `python -m venv .venv`

Type Checking

- [MUSS]: Eine konsequente Typisierung von Variablen und Funktionen (Type Hints) und dies automatisiert zu Testen ist verpflichtend für Produktivsysteme.
- [EMPFOHLEN]: Automatisiertes Testen der Typisierung mittels `mypy`.

- [KANN]: Prototypische Projekte können mit Begründung auch ohne `mypy` entwickelt werden.

Web/API Frameworks

- [EMPFOHLEN]: Django ist das bevorzugte Framework zur Entwicklung von webbasierten Applikationen und APIs. Hierbei sind die djangospezifischen Best Practices verpflichtend.
- [KANN]: FastAPI, Flask sind zulässig, wenn die Entscheidung auf einer fundierten Architekturentscheidung (z. B. Microservices) beruht.

Network Programming

- [EMPFOHLEN]: Twisted.

Style Guide Anwendung

Folgende Developer Libraries unterstützen die Anwendung des PEP8 Style Guides im Projekt:

- [MUSS]: `pylint` - Statische Codeanalyse.
- [MUSS]: OS- und plattformübergreifende Workspace Parameter müssen in einer Editorconfig gepflegt werden.
- [MUSS]: Code Formatierung:
  - [EMPFOHLEN] `black`
  - [KANN] Flake8 - kombiniert PEP8, PyFlakes und zirkuläre Komplexität.
- [EMPFOHLEN]: `mypy` - Optional Static Typing in Python.
- [EMPFOHLEN]: `semgrep` - Tool zur statischen Codeanalyse.
- [EMPFOHLEN]: `isort` - automatisiertes Ordnen/Formatieren von imports.
- [EMPFOHLEN]: `pre-commit` - Problemidentifizierung vor Code commits.
- [EMPFOHLEN]: Sphinx mit `rtd-theme plugin` - Tool zur automatischen Generierung von Dokumentationen.

Folgende Konfigurationen können bzw. müssen für PyLint / Black angewendet werden:

- [MUSS]: Maximale Zeilenlänge 100.
- [EMPFOHLEN]: Keine Docstrings in Test-Modulen und -Klassen erzwingen.

EditorConfig (im Anhang)

```
root = true

[*.py]
charset = utf-8
end_of_line = lf
indent_style = space
indent_size = 4
trim_trailing_whitespace = true
insert_final_newline = true
```

`

Testing Frameworks

- [MUSS]: `pytest` ist als Testrunner zu verwenden.
- [EMPFOHLEN]: Pytest Testing Framework sollte genutzt werden.
- [KANN]: `unittest` kann verwendet werden, da es auch durch den `pytest testrunner` ausführbar ist.

Kommentare & Dokumentation

- [EMPFOHLEN]: Kommentieren einzelner Funktionen und Klassen mit Docstrings nach PEP 257 im Numpy-Docstring-Format.
- [EMPFOHLEN]: (Entwickler-)Dokumentation der Software (z. B. mit Sphinx oder MKDocs).

3.3.8 Swift

Ansprechpartner: Frank Rotermund, BWI

Diese Coding Guideline dient gemeinsam mit der allgemeinen Guideline als Leitfaden für die Entwicklung mit den Programmiersprachen Swift und Objective-C für iOS- und MacOS-Anwendungen.

Coding Guide Grundlage

- [MUSS]: Als generelle Basis an Richtlinien wird die Swift Design Guideline festgelegt.

IDE

- [MUSS]: XCode. Die Verwendung anderer IDEs bietet Umsteigern zwar einen schnelleren Zugang, stellt aber eine zusätzliche Fehlerquelle dar.
- [EMPFOHLEN]: Es sollte immer die aktuelle stabile Version von XCode genutzt werden.

Formatierung

- [EMPFOHLEN]: Bei neuen Projekten sind die durch XCode per default vorgegebenen Formatierungsregeln für Swift zu verwenden.
- [EMPFOHLEN]: Editorconfig wird durch XCode nicht nativ unterstützt und sollte nicht genutzt werden.

Objective-C

- [MUSS]: Zur Entwicklung neuer Projekte und Komponenten soll Swift genutzt werden mit folgenden Ausnahmen:
  - [EMPFOHLEN]: zur Anpassung von vorhandenem Legacy Quellcode. Dabei gelten die Style-Richtlinien des jeweiligen Legacy Quellcodes.
  - [KANN]: für Algorithmen, deren Performance mit Objective-C deutlich besser ist, als mit Swift.

Testing

- [EMPFOHLEN]: Unit Tests sollten mit dem XCTest Framework geschrieben werden.

3.4 Coding Process

Dieses Kapitel enthält Vorgaben und Informationen zum Konfigurationsmanagement. Es steht im Einklang mit den Architekturprinzipien der BWI: AP04 Beherrschbarkeit, AP07 Erweiterbarkeit, AP09 Robustheit, AP12 Skalierbarkeit und AP13 Standardisierung.

3.4.1 Configuration Management

Ansprechpartner: Guido Wojke, BWI

Dieses Kapitel betrachtet den Teil des Konfigurationsmanagements, der für die Erstellung von Softwareprodukten und zugehörigen Server-bzw. Cluster-Konfigurationen notwendig ist.

Definition **Konfigurationsmanagement** (nach ISO 10007): Konfigurationsmanagement "ist eine Managementtätigkeit, die die technische und administrative Leitung des gesamten Produkt- und Dienstleistungslebenszyklus, dessen Konfigurationsangaben und Status und der produkt- und dienstleistungskonfigurationsbezogenen Angaben übernimmt."

Alle Änderungen an Konfigurationen des Builds und der erzeugten Artefakte müssen über eine Versionskontrolle (siehe Kapitel Version Control) nachvollziehbar sein. Auch bei Server- bzw. Cluster-Konfigurationen ist deren Versionierung empfohlen. Diese Konfigurationen werden entweder mit dem Quellcode oder in einem separaten Projekt in der Versionskontrolle versioniert. Es darf keine Änderung außerhalb der Versionskontrolle geschehen.

[MUSS]: Verpflichtende Aktivitäten

- Nutzung der Versionskontrolle, um Build-Konfigurationen der Softwareprodukte zu dokumentieren.
- Nutzung eines Build-Werkzeugs, um das Softwareprodukt zu erstellen.
- Nutzung der Versionskontrolle, um CI/CD-Konfigurationen der Softwareprodukte zu dokumentieren.
- Nutzung eines CI-Servers, um das Softwareprodukt kontinuierlich zu erstellen.
- Nutzung eines Artefaktspeichers / Repositorymanagers, um erstellte Softwareprodukte zu archivieren.

[EMPFOHLEN]: Optionale Aktivitäten

- Nutzung der Versionskontrolle, um Server-Konfigurationen zu dokumentieren.
- Nutzung von Werkzeugen zum Ausrollen von Server-Konfigurationen.
- Nutzung der Versionskontrolle, um Cluster-Konfigurationen zu dokumentieren.
- Nutzung von Werkzeugen zum Ausrollen von Cluster-Konfigurationen.
- Konfigurationsdateien sowohl in der Anzahl als auch in der Komplexität möglichst gering halten.

Weiterführende Information - Werkzeuge zur Server-Konfiguration

Werkzeuge zum Ausrollen von Server-Konfigurationen können u.a. sein

- Ansible
- Puppet
- Chef
- Saltstack

Bei einer Entscheidung, welches Werkzeug zum Einsatz kommt, sind Werkzeuge zu bevorzugen, die keine zusätzliche Software auf dem Zielsystem benötigen.

Weiterführende Information - Werkzeuge zur Cluster-Konfiguration / Delivery

Werkzeuge zum Ausrollen von Cluster-Konfigurationen können u.a. sein

- Helm
- Kustomize
- ArgoCD

3.4.1.1 Configuration Management mit Ansible

Ansprechpartner: Guido Wojke, BWI

Red Hat® Ansible®

Red Hat® Ansible® ist eine agentenlose Software, um Konfiguration auf Rechnern automatisiert auszubringen.

Beim Einsatz dieser Software gelten folgende Regeln:

- [MUSS]: Der Code muss im Versionskontrollsystem abgelegt sein.
- [MUSS]: Die Codestruktur folgt dem Ansible® Sample setup.
- [MUSS]: Geheimnisse im Code müssen mit einem außerhalb des Versionskontrollsystem abgelegten Schlüssel mit ansible-vault verschlüsselt sein.
- [MUSS]: Es ist ansible-lint zu verwenden und die Regeln müssen eingehalten werden.
- [EMPFOHLEN]: Plays und Rollen müssen sprechende Namen haben.
- [EMPFOHLEN]: Wiederverwendbare Rollen sind in eigene Repositories ausgelagert.
- [EMPFOHLEN]: Wiederverwendbare Rollen sind mit Ansible Molecule getestet.
- [EMPFOHLEN]: Wiederverwendbare Rollen haben sinnvolle default Werte und sind ohne Überschreiben von Variablen lauffähig.
- [EMPFOHLEN]: Beachtung der Idempotenzregeln in allen Tasks (insbesondere bei Verwendung der Module ansible.builtin.shell bzw. ansible.builtin.command).

IDE für Red Hat ® Ansible®

Beim Entwickeln von Code mit Ansible können folgende Entwicklungsumgebung und Erweiterungen genutzt werden:

- [EMPFOHLEN]: IDE: Microsoft Visual Studio Code
- [EMPFOHLEN]: Sprachunterstützung für YAML: YAML Language Support by Red Hat®
- [EMPFOHLEN]: Ansible® Erweiterung für Visual Studio Code: Ansible VS Code Extension by Red Hat®

YAML in Red Hat ® Ansible®

- [MUSS]: Die Einrücktiefe für jede Ebene im Code beträgt 2.
- [MUSS]: Kommentare beginnen mit # auf der gleichen Ebene wie die Codezeilen.
- [MUSS]: Wahrheitswerte werden ausschließlich mit **true** bzw. **false** gesetzt.
- [MUSS]: Mehrzeilige Texte müssen im "Literal Block Scalar Style" **|** oder "Folded Block Scalar Style" **>** geschrieben werden.

YAML Beispiele

```yaml
# Comment and list example
values:
  example_string: "Oneliner with spaces"
  example_list:
    # Comment
    - one: true
    - two: false
    # - three: unknown
    - four: true
```

```yaml
include_newlines: |
  exactly as you see
  will appear these three
  lines of poetry

fold_newlines: >
  this is really a
  single line of text
  despite appearances
```

3.4.2 Version Control

Ansprechpartner: Guido Wojke, BWI

Gemäß CON.8.A10 ist in allen Softwareprojekten ein Versionskontrollsystem für Source Code zu verwenden. Die SDE stellt hierfür ein zentral verwaltetes Git zur Verfügung (siehe Kapitel Technology). Bei der Verwendung des Gits ist generell Folgendes zu beachten:

- [MUSS]: Es muss eins der folgenden Branching-Modelle eingesetzt werden.
  - [EMPFOHLEN]: Das empfohlene Branching-Modell ist GitFlow, geeignet vor allem in der App-Entwicklung oder allgemein bei Produkten, bei denen Änderungen durch einen Review-Prozess nicht automatisch und unmittelbar veröffentlicht werden können.
  - [KANN]: Für Produkte mit automatisierter und kontinuierlicher Veröffentlichung kann auch alternativ ein trunk-based Modell verwendet werden.
- [MUSS]: Fertig gebaute Softwareartefakte (generierte Dateien und Binärartefakte) dürfen **nicht** in der Versionskontrolle abgelegt werden. Für diese Softwareartefakte steht ein Artefaktspeicher / Repositorymanager zur Verfügung.
- [MUSS]: Für große Binärdateien (> 5 MebiByte) ist Git Large File Storage (LFS) sowohl auf dem Remote Repository als auch in allen Clients zu benutzen.
- [EMPFOHLEN]: Für Binärdateien (<= 5 MebiByte) ist Git Large File Storage (LFS) sowohl auf dem Remote Repository als auch in allen Clients zu benutzen.

Anmerkung: Für ältere bzw. Legacy-Projekte wird teilweise der alte Name "master" (anstelle von "main") für den Haupt-Branch verwendet.

GitFlow Branches

- [MUSS]: Der Main Branch ist geschützt. Änderungen müssen über Merges von Release & Hotfix Branches vorgenommen werden.
- [EMPFOHLEN]: Der Develop Branch soll nur über Merges von Feature, Release & Hotfix Branches geändert werden.
- [MUSS]: Release und Hotfix Branches folgen dieser Notation: (release|bugfix)/<VersionsTag>
- [MUSS]: Feature Branches folgen dieser Notation: feature/<Jira issue - nur Nummer>_<Kurzbeschreibung>

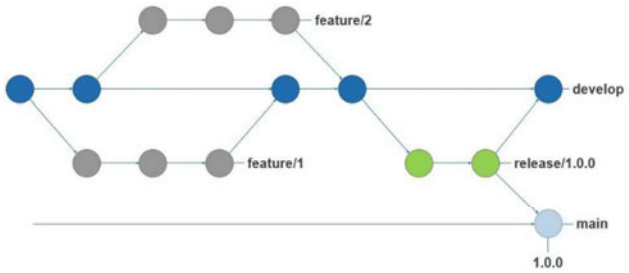


Abbildung: GitFlow Branching-Modell

trunk-based Branches

- [MUSS]: Die Entwicklung findet auf dem Main Branch ("main") statt.
- [MUSS]: Nutzung von Feature Branches (scaled trunk-based Ansatz). Diese Branches folgen der Notation: feature/<Jira issue - nur Nummer>_<Kurzbeschreibung> und sind schnell abzuschließen (z. B. innerhalb eines Sprints oder kürzer).
- [KANN]: Nutzung von Release Branches (z. B. als Branch für QA). Diese Branches folgen dieser Notation: release/<VersionsTag>

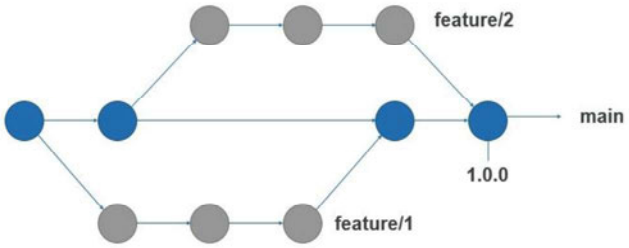


Abbildung: trunk-based Branching-Modell

Tags

- [MUSS]: Versionen werden auf dem *main* getaggt (lightweight, bei GitFlow kann dies automatisiert erfolgen). Nur getaggte Versionen werden ausgeliefert.
- [EMPFOHLEN]: Sofern vorhanden können noch Metainformationen (z. B. Release-Informationen) zum Tag (annotated) hinzugefügt werden.

Commit-Nachrichten

- [MUSS]: Commits folgen dieser Notation: <Jira Issue mit Projektname> - <commit message> also z. B. MESSENGER-1635 fixed wrong password
- [EMPFOHLEN]: Die Benennung der Commit-Nachrichten sollte in der Sprache erfolgen in der die User Stories geschrieben sind.

Merge Request/Code Review

- [MUSS]: Jede Code-Änderung findet auf einem dedizierten Branch statt und nicht auf dem produktiven Stand (main / master).
- [MUSS]: Für jeden Branch, der nach *develop* oder *main* gemergt wird, muss ein Merge Request (mit Merge Commit als Merge Methode) geöffnet und an ein anderes Teammitglied (idealerweise Senior Entwickler*in) zum Code Review weitergeleitet werden.
- [MUSS]: Das andere Teammitglied muss den Merge Request umgehend zurückweisen, wenn die Richtlinien aus diesem Dokument nicht eingehalten werden (teilweise automatisiert überprüft).
- [MUSS]: Jeder Code Review muss protokolliert werden. Zu empfehlen ist dabei eine automatische Protokollierung während Einsatz eines Tools zur Abwicklung von Merge Requests, z. B. Gitlab.
- [EMPFOHLEN]: Die Branches sollten nicht für lange Zeit (z. B. nicht über mehrere Sprints hinweg) geöffnet bleiben. Die Änderungen sollten klein gehalten werden und größere Änderungen in mehrere kleine Teile zerlegt werden.
- [EMPFOHLEN]: Commits sollen bei der Durchführung eines Merge Requests gesquasht werden.

Unversionierte Dateien

- [MUSS]: Temporäre Dateien, lokale Konfigurationen, bei jedem Build-Prozess generierter Code und Binärdateien dürfen nicht in Git eingecheckt werden.
- [MUSS]: Userspezifische Ordner und Dateien sind in der *.gitignore* Datei zu vermerken.
- [MUSS]: In jeder Sprache gibt es weitere programmiersprachenspezifische Ordner und Dateien, für die keine Versionskontrolle notwendig ist. Diese müssen auch in der *.gitignore* vermerkt werden. Hierfür kann auf fertige Templates für viele Programmiersprachen und IDEs zurückgegriffen werden.

Workflow-Erweiterungen

- [EMPFOHLEN]: Falls langlaufende Versionen notwendig sind (z. B. bei Nutzung einer alten Version nach Erscheinen einer neuen Version), sollten diese in Support Branches abgelegt werden (support/<versionTag>). Änderungen in Support Branches werden, falls nötig, per Cherrypick in den Hauptentwicklungszweig *(main* bzw. *develop)* überführt.

3.5 Software Quality & Assurance

Ansprechpartner: Berno Kneer, BWI; Guido Wojke, BWI; Dominik Röser, ZDigBw

Dieses Kapitel beschreibt die verpflichtenden Prozessschritte, hohe Software-Produktqualität sicherzustellen. Dieses Kapitel entspricht den Vorgaben CON.8.A7. Einige grundlegende Definitionen und Hintergrundwissen zum Thema Software Quality & Assurance sind im Glossar abgelegt.

Zusammenfassung:

- Für alle Projekte ist ein Testkonzept zu erstellen.
- Von diesem Testkonzept wird ein Testplan abgeleitet.
- Das Testing der Software bzw. des Produkts findet kontinuierlich parallel zur Entwicklung und nicht als festgelegte Phase (z. B. am Ende der gesamten Entwicklung) statt.
- Der Testprozess beinhaltet sowohl die Planung als auch den Entwurf und die Entwicklung der Tests.
- Dazu kommen statische und dynamische Tests auf allen Teststufen zum Einsatz.
- Jede Änderung an diesen Prozessen und Dokumenten muss dokumentiert werden.
- Für Software-Qualitätsrelevante Begriffe werden die Definitionen gemäß ISTQB verwendet.

3.5.1 Software Quality

Definition (Software-) Qualität (nach ISTQB): Der Grad, in dem ein System, eine Komponente oder ein Prozess die Kundenerwartungen und -bedürfnisse erfüllt (Ref: ISO 24765). Dabei werden funktionale (explizite) und nicht-funktionale (implizite) Anforderungen unterschieden. Die Erfüllung der Anforderungen werden durch ein Qualitätsmanagement sichergestellt, welches Aktivitäten in den Bereichen Software-Qualitätssicherung (Software Quality Assurance, SQA), Software-Qualitätskontrolle (Software Quality Control, SQC) und Softwaretests (Testing) umfasst.

QA, QC and Testing in software development process

Bildquelle:https://www.altexsoft.com/whitepapers/quality-assurance-quality-control-and-testing-the-basics-of-software-quality-management/

Zu verwendende Standards

- Die möglichen Vorgehensweisen sind im Kapitel Methodology definiert. SQA, SQC und Testing sind Bestandteil jeder dieser Methoden. Empfohlen wird eine agile Methode.
- SQA, SQC und Testing verwenden für alle Begriffe die Definitionen gemäß ISTQB.

3.5.2 Software Quality Assurance (SQA)

Definition **(Software-) Qualitätssicherung** (nach ISTQB): Aktivitäten, die darauf fokussieren, Vertrauen in die Erfüllung der Qualitätsanforderungen zu erzeugen.

Weiterführende Informationen - SQA

Die Software-Qualitätssicherung umfasst den gesamten Lebenszyklus der Softwareentwicklung und soll sicherstellen, dass die Entwicklungs- und Wartungsprozesse kontinuierlich verbessert werden, um Produkte zu erzeugen, die den Spezifikationen entsprechen. Zu beachten ist, dass der Bereich Software-Qualitätssicherung nicht nur auf Softwaretests beschränkt ist. Die Rolle der SQA besteht darin, die Art und Weise zu überwachen, wie ein Projekt seine Aufgaben erfüllt. Sie konzentriert sich also mehr auf die organisatorischen Aspekte des Qualitätsmanagements, ist prozessorientiert und gilt für alle Projekte innerhalb der Abteilung.

Typische Aktivitäten der SQA:

- Audits.
- Schulungen.
- Prozess-Definition und -Implementierung.
- Kontrolle extern zur Verfügung gestellter Services und Produkte (Software).
- Standardisierung.

[MUSS]: Verpflichtende Aktivitäten

- Erstellung des Testkonzepts.
- Festlegung der Kommunikations- und Dokumentationsvorgaben.
- Festlegung von Reviews und Audits (welche und in welcher Häufigkeit).
- Prüfung extern zur Verfügung gestellter Services und Produkte (Vendor Management).
- Festlegung der Arbeitsergebnisse (Work Products).
- Definition der Zusammenarbeit mit dem Kunden.
- Definition der Eskalationsmöglichkeiten und -kanäle.

[EMPFOHLEN]: Optionale Aktivitäten

- Erstellung eines Schulungsplans für die Tester*innen/Entwickler*innen.

Weiterführende Informationen - Testkonzept

Definition **Testkonzept** (nach ISTQB): Ein Dokument, das u.a. den Gültigkeitsbereich, die Vorgehensweise, die Ressourcen und die Zeitplanung der beabsichtigten Tests mit allen Aktivitäten beschreibt. Es identifiziert u.a. die Testobjekte, die zu testenden Features und die Testaufgaben. Es ordnet den Testaufgaben die Tester*innen zu und legt den Unabhängigkeitsgrad der Tester*innen fest. Es beschreibt die Testumgebung, die Testentwurfsverfahren und die anzuwendenden Verfahren zur Messung der Tests, und begründet deren Auswahl. Außerdem werden Risiken beschrieben, die eine Planung für den Fall des Eintretens erfordern. Ein Testkonzept ist somit die Niederschrift des Testplanungsprozesses.

Gliederung Testkonzept nach IEEE 829-1998:

1. Testkonzeptbezeichnung.
2. Einführung.
3. Testobjekte.
4. Zu testende Leistungsmerkmale.
5. Leistungsmerkmale, die nicht getestet werden.
6. Teststrategie.
7. Abnahme- und Ausgangskriterien.
8. Kriterien für Testabbruch und Testfortsetzung.
9. Testdokumentation.
10. Testaufgaben.
11. Testinfrastruktur.
12. Verantwortlichkeiten/Zuständigkeiten.
13. Personalprofil, Einarbeitung.
14. Zeitplan/Arbeitsplan.
15. Planungsrisiken und Unvorhergesehenes.
16. Genehmigung/Freigabe.

(Quelle: Andreas Spillner und Tilo Linz, Basiswissen Softwaretest, dpunkt.verlag)

Zu verwendende Standards

Die folgenden Standards bez. SQA sind weit verbreitet, sind aber (noch) nicht an agile Methoden angepasst. Trotzdem bieten sie eine gute Orientierung, sind aber innerhalb des SWE Frameworks nicht verpflichtend:

- ISO 9000: Basiert auf sieben Qualitätsmanagement-Prinzipien, die sicherzustellen sollen, dass Produkte/Dienstleistungen auf die Bedürfnisse der Kunden abgestimmt sind.
- CMMI (Capability Maturity Model Integration): Ziel von CMMI-Modellen ist es, Prozesse in einem Projekt, einer Abteilung oder einer Organistion zu verbessern. Wie weit fortgeschritten man ist, wird in 5 Reifegraden gemessen.
- TMMI (Test Maturity Model Integration): Basiert auf CMMI und konzentriert sich auf auf Software-Qualitätsmanagement und -Testen.

3.5.3 Software Quality Control (SQC)

Definition **(Software-) Qualitätskontrolle (SQC)**(nach ISTQB): Eine Menge von Aktivitäten, die entworfen wurde, um die Qualität einer Komponente oder eines Systems zu bewerten.

Der Prozess der Software-Qualitätskontrolle (SQC) wird von der Software-Qualitätssicherung (SQA) gesteuert.

Weiterführende Informationen - SQC

Während SQA auf die Vorbeugung ausgerichtet ist, ist SQC auf die Entdeckung ausgerichtet. SQC ist projekt- bzw. produktspezifisch. Durch die Qualitätskontrolle wird geprüft, ob das Produkt die Anforderungen erfüllt. Ziel ist es, die Produktqualität beizubehalten oder zu verbessern, indem Fehler (z. B. Fehlfunktionen, Risiken, Abweichungen von der Spezifikation) möglichst frühzeitig erkannt und beseitigt werden.

[MUSS]: Verpflichtende Aktivitäten

- Erstellung des Testplans.
- Durchführen und Dokumentieren von Reviews:
  - Architektur und Design Review.
  - Code Review.
  - Test Cases Review.
- Durchführen von Tests: Unit Testing, Integration Testing, System Testing, Acceptance Testing.
- Testdurchführung in Test- und Entwicklungsumgebungen, die vollständig getrennt von der Produktivumgebung sind.
- Dokumentation der Testergebnisse.
- Bewertung von Change Requests.
- Definieren und Auswerten der projektspezifischen Metriken.
- Überprüfung der Konsistenz der Daten.
- Überprüfung der korrekten Weitergabe von Daten zwischen Verarbeitungsschritten.
- Überprüfung, ob die Systemvoraussetzungen für die vorgesehene Software ausreichend dimensioniert sind.
- Erstellung von Fehlerberichten (Ticket).

[EMPFOHLEN]: Optionale Aktivitäten

- Durchführen und Dokumentieren von Reviews:
  - Requirement Reviews.
  - Deployment Plan Review.
  - Test Plan Review.
- Rückverfolgung von Requirements.
- Aktionen zur Risikobewältigung.
- Vergleich der Ergebnisse mit früheren Ergebnissen.
- Einbindung der Fachverantwortlichen oder der beauftragenden Fachabteilung (Auftraggeberseite).
- Definition der Testdaten (z. B. Grenzwerte, kritische Werte).

Weiterführende Informationen - Testplan

Definition **Testplan** (nach ISTQB): Eine Liste von Aktivitäten, Aufgaben oder Ereignissen des Testprozesses, mit Angabe ihrer geplanten Anfangs- und Endtermine sowie ihrer gegenseitigen Abhängigkeiten.

Ein Testplan enthält:

- Schedules.
- Konkrete Beschreibung der Testumgebungen.
- Konkrete Beschreibung der Test-Entwicklungsumgebungen (Hardware Requirements, Software Requirements, Netzwerkanbindung, etc.).
- Konkrete Beschreibung, welche Testarten in welcher Teststufe in welcher Umgebung zum Einsatz kommen.
- Konkrete Beschreibung der Teststufen.
- Abhängigkeiten.

Zu verwendende Standards

- In der BWI wird die Plan-Do-Check-Act-Methode (PDCA-Methode) verwendet.

3.5.4 Softwaretests (Testing)

Definition **Testing** (nach ISTQB): Der Prozess, der aus allen statischen und dynamischen Lebenszyklusaktivitäten besteht, die sich mit der Planung, Vorbereitung und Bewertung einer Komponente oder eines Systems und zugehörigen Arbeitsergebnissen befassen, um festzustellen, ob sie festgelegte Anforderungen erfüllen, für den Zweck geeignet sind sowie um etwaige Fehlerzustände zu finden.

Beim Testen von Software müssen die sieben Grundsätze des Softwaretestens beachtet werden:

Die 7 Grundsätze des Softwaretestens

1. **Testen zeigt die Anwesenheit von Fehlerzuständen, nicht deren Abwesenheit:**

Testen kann zeigen, dass Fehlerzustände vorliegen, aber es kann nicht beweisen, dass es keine Fehlerzustände gibt. Testen reduziert die Wahrscheinlichkeit, dass noch unentdeckte Fehlerzustände in der Software vorhanden sind, aber auch wenn keine Fehlerzustände gefunden werden, ist Testen kein Beweis für Korrektheit.

2. **Vollständiges Testen ist nicht möglich**

Ein vollständiger Test, bei dem alle möglichen Eingabewerte und deren Kombinationen unter Berücksichtigung aller unterschiedlichen Vorbedingungen ausgeführt werden, ist nicht durchführbar, mit Ausnahme von sehr trivialen Testobjekten. Anstatt zu versuchen, vollständig zu testen, sollten Risikoanalyse, Testverfahren und Prioritäten genutzt werden, um den Testaufwand zu konzentrieren.

3. **Frühes Testen spart Zeit und Geld**

Um Fehlerzustände früh zu finden, sollten sowohl statische als auch dynamische Testaktivitäten so früh wie möglich im Softwareentwicklungslebenszyklus gestartet werden. Frühes Testen wird oft als Shift left bezeichnet. Frühes Testen im Softwareentwicklungslebenszyklus hilft dabei, kostenintensive Änderungen zu reduzieren oder vollständig zu vermeiden.

4. **Häufung von Fehlerzuständen**

Eine kleine Anzahl von Modulen enthält in der Regel die meisten Fehlerzustände, die während des Testens in der Phase vor Inbetriebnahme entdeckt werden, oder ist verantwortlich für die meisten der betrieblichen Fehlerwirkungen. Vorausgesagte Anhäufungen von Fehlerzuständen und die tatsächlich beobachteten Anhäufungen von Fehlerzuständen im Test oder im Betrieb sind ein wichtiger Beitrag zur Risikoanalyse, die genutzt wird, um den Testaufwand zu konzentrieren (wie in Grundsatz 2 erwähnt).

5. **Vorsicht vor dem Pestizid-Paradoxon**

Wenn die gleichen Tests immer wieder wiederholt werden, finden diese Tests irgendwann keine neuen Fehlerzustände mehr. Um neue Fehlerzustände zu finden, müssen bestehende Tests und Testdaten möglicherweise verändert werden und neue Tests geschrieben werden (Tests sind nicht länger effektiv im Erkennen von Fehlerzuständen, so wie Pestizide nach einer Weile nicht mehr effektiv in der Vernichtung von Insekten sind). In manchen Fällen, wie dem automatisierten Regressionstest, hat das Pestizid-Paradoxon einen vermeintlich positiven Effekt, der in der relativ geringen Anzahl von Regressionsfehlern liegt.

6. **Testen ist kontextabhängig**

Je nach Einsatzgebiet und Kontext ist das Testen anzupassen. Zum Beispiel wird sicherheitskritische industrielle Steuerungssoftware anders getestet als eine mobile E-Commerce-Applikation. Ein weiteres Beispiel ist das Testen in agilen Projekten, das anders durchgeführt wird als das Testen in einem Projekt mit sequenziellem Softwareentwicklungslebenszyklus.

7. **Trugschluss: „Keine Fehler“ bedeutet ein brauchbares System**

Einige Unternehmen erwarten, dass Tester*innen alle denkbaren Tests durchführen und alle denkbaren Fehlerzustände finden können, aber die Grundsätze 2 und 1 lehren uns, dass dies unmöglich ist. Des Weiteren ist es ein Trugschluss (d.h. ein Irrglaube), zu erwarten, dass allein das Finden und Beheben einer großen Anzahl von Fehlerzuständen den Erfolg eines Systems sicherstellen werde. Beispielsweise kann trotz gründlicher Tests aller spezifizierten Anforderungen und Beheben aller gefundenen Fehlerzustände ein System erstellt werden, das schwer zu nutzen ist, das die Bedürfnisse und Erwartungen der Benutzer*innen nicht erfüllt oder das geringwertigere Qualität hat als vergleichbare Systeme.

[MUSS]: Verpflichtende Aktivitäten

- Es müssen Testfälle auf allen Teststufen erstellt werden.
- Es dürfen alle Testarten (Funktional/Nichtfunktional/...) benutzt werden, wobei sowohl die funktionalen als auch die nichtfunktionalen Anforderungen geprüft werden müssen.
- Softwaretests müssen auch Negativtests abdecken.

- Kritische Grenzwerte bez. Eingabe und Datentypen müssen geprüft werden.
- Durchführung von statischen und dynamischen Tests inkl. Erfassung der Metriken.
- Metriken:
  - Es gelten die Quality Profiles und Quality Gates der BWI in der jeweilig genutzten Technologie. Diese sind im DevLab bereits standardmäßig hinterlegt und können bei Bedarf bei den Kapitelverantwortlichen angefragt werden.
  - Diese Quality Profiles und Quality Gates werden von der BWI zweimal jährlich geprüft und ggf. angepasst.
  - Die Quality Profiles und Quality Gates liegen in einer digitalen Form vor.
  - Ausnahmen müssen beim Review abgenommen werden.
- Durchführen von Regressionstests.
- Mindestens ein Test pro funktionaler Anforderung.
- Mindestens ein Test pro behobenem Fehler aus einem Fehlerbericht.
- Testprotokolle für produktive Versionen müssen revisionssicher abgelegt werden.
- Erstellung und Pflege eines Testfallkatalogs.

[EMPFOHLEN]: Optionale Aktivitäten

- Anwendung des "Test first"-Paradigmas.
- Automatisierte Ausführung aller Tests.

Hinweise zu Testfällen:

Definition Testfall (nach ISTQB): "Eine Menge von Vorbedingungen, Eingaben, Aktionen (falls anwendbar), erwarteten Ergebnissen und Nachbedingungen, welche auf Basis von Testbedingungen entwickelt wurden."

Ein Testfall muss mindestens folgende Dinge beinhalten:

- Vorbedingungen: Welche Voraussetzungen müsssen erfüllt sein, damit der Test durchgeführt werden kann? Dies können technische und organisatorische Dinge sein. Wenn diese erfüllt sind, darf der Test nicht fehlschlagen.
- Testdaten: Welche Daten müssen im Testsystem vorhanden sein und welche Eingaben werden gemacht?
- Testschritte: Welche Aktionen werden in welcher Reihenfolge durchgeführt?
- Erwartetes Ergebnis: Welche Reaktion wird vom System erwartet? Dies sollte pro Testschritt definiert werden, muss aber mindestens für den Testfall definiert sein.
- Nachbedingungen: Erwartete Nachbedingungen/Ergebnisse der Testdurchführung, z. B. "Benutzer ist erfolgreich angemeldet".

Zu verwendende Standards

Der folgende Standard gibt eine gute Orientierung, ist aber im Rahmen des SWE Frameworks nicht verpflichtend:

- ISO 25010: Beschreibt acht Qualitätsmerkmale, die bei der Prüfung eines Softwareprodukts berücksichtigt werden sollen.

Fehlerpriorität und Fehlerklassen

Während die Fehlerpriorität bzw. Prioritätsklasse beschreibt, wie dringend ein Fehler behoben werden, beschreibt die Fehlerklasse, wie schwerwiegend ein Fehler ist, d.h., wie stark er die Nutzung beeinträchtigt (Grad der Behinderung des Produkteinsatzes). Da die Fehlerpriorität und die Fehlerklasse nicht immer korrelieren, müssen beim Erfassen von Fehlertickets beide erfasst werden.

Es wird zwischen fünf Prioritätsklassen unterschieden:

- Prio 1 (Patch): Der Arbeitsablauf bei Anwender*in/Tester*in ist blockiert oder die laufenden Tests können nicht fortgesetzt werden. Das Problem muss unmittelbar, ggf. provisorisch, behoben werden. Ein Patch ist zu erstellen.
- Prio 2 (Nächste Version): Die Fehlerkorrektur erfolgt mit der nächsten produktiven Produktversion.
- Prio 3 (Übernächste Version): Die Fehlerkorrektur erfolgt (spätestens) mit der übernächsten produktiven Produktversion.
- Prio 4 (Gelegentlich): Die Fehlerkorrektur erfolgt, sobald die betroffenen Systemteile ohnehin überarbeitet werden.
- Prio 5 (Offen): Es gibt keinen Zeitplan für die Fehlerkorrektur.

Es wird zwischen fünf Fehlerklassen unterschieden:

Fehlerklasse	Definition	Beispiele
1 - (Blocker/Kritisch)	▪ Die App ist in dieser Form nicht einsetzbar.	▪ App stürzt rekonstruierbar oder häufig ab. ▪ App kann nicht benutzt werden (z. B. weil ein Dialog die App blockiert). ▪ Wichtiges Feature funktioniert nicht und es gibt keinen Workaround.
2 - (Hoch)	▪ Eine wesentliche Funktion ist fehlerhaft. ▪ Eine Anforderung wurde nicht beachtet oder falsch umgesetzt. ▪ Die App ist nur mit großen Einschränkungen einsetzbar.	▪ Die App stürzt nicht rekonstruierbar und selten ab. ▪ Ein wichtiges Feature funktioniert nicht, kann aber über einen Workaround genutzt werden.
3 - (Normal/Medium)	▪ Funktionale Abweichung bzw. Einschränkung. ▪ Anforderung fehlerhaft oder nur teilweise umgesetzt.	▪ Es wurden nicht alle Regeln zur Passwortvergabe umgesetzt. ▪ Die Sortierung einer Liste erfolgt nach Vorname und nicht nach Nachname.

Fehlerklasse	Definition	Beispiele
	▪ Die App kann mit Einschränkungen genutzt werden.	
4 - (Niedrig)	▪ Geringfügige Abweichung. ▪ Die App kann ohne Einschränkung genutzt werden.	▪ Eine Liste zeigt statt maximal 10 Einträgen bis zu 15 an. ▪ Eine Fehlermeldung ist nicht klar verständlich.
5 - (Kosmetisch)	▪ Schönheitsfehler. ▪ Die App kann ohne Einschränkung genutzt werden.	▪ Rechtschreibfehler. ▪ Mangel im Maskenlayout.

Testprotokolle

Testprotokolle für ausgeführte Tests (manuell oder automatisiert) müssen so abgelegt werden, dass die Historie der Testausführungen jederzeit nachvollziehbar ist. Da Testprotokolle meist auch Liefergegenstände sind, empfiehlt es sich, diese zusammen mit der Projekt-/Produkt-dokumentation abzulegen.

Inhalt eines Testprotokolls

- Testobjekt
  - Eindeutige Identifikation der getesteten Software (z. B. Versionsnummer, Build, Bezeichnung der Baseline).
- Testumgebung
  - Bezeichnung.
  - Spezielle Einstellungen / Konfigurationen.
- Testprogramme
  - Testsoftware inkl. Version.
- Testdurchführung
  - Datum und ggf. Uhrzeit.
  - Wer hat den Test durchgeführt?
  - Ablageort des Testprotokolls.
- Informationen zu jedem einzelnen Test:
  - Test-ID und Bezeichnung.
  - Testergebnis.
  - (Optional) Bewertung und Bemerkungen. Empfohlen bei fehlgeschlagenen Tests.

Security Tests

Im Rahmen von den notwendigen Security-by-Design- and Development-Tätigkeiten werden Security-bezogene Tests durch die Entwicklungsteams durchgeführt. Um die Qualität zu steigern, kann ein unabhängiges (Entwicklungs)team beauftragt werden. Eine offizielle Abnahme für die Sicherheit des Produktes erfolgt entweder durch CCITS als Facheinheit oder durch beauftragte Dritte (spezialisierte Industrieunternehmen).

Weiterführende Links

- ISTQB Referenz
  - https://www.german-testing-board.info/wp-content/uploads/2020/01/CTFL-DE_Syllabus_2018_V3.1.pdf
  - https://www.german-testing-board.info/wp-content/uploads/2016/07/Certified-Tester-Foundation-Level-Extension-Deutsch.pdf

4 Software Operating Module

Das Software Operating Module beschreibt, wie die eigenentwickelte Software in den BWI-Betrieb überführt und anschließend aus Softwareentwicklungssicht begleitet wird. Dazu zählen Deployment, Operating, Monitoring & Reporting sowie Maintenance & Support. Das Modul beinhaltet ein Kapitel mit allgemeinen Vorgaben sowie Kapitel zu den einzelnen Zielplattformen mit spezifischen Vorgaben.

4.1 Allgemeine Operating Vorgaben

Ansprechpartner: Burkhard Pietsch, BWI; Günter Liehl, BWI

Dieses Kapitel enthält Vorgaben aus Softwareentwicklungssicht für den Betrieb von eigenentwickelter Software in der BWI. Die Vorgaben in diesem Kapitel sind unabhängig von dem Betriebsmodell (Server, Cloud, Desktop und Mobile) und werden, abhängig von den technologischen und organisatorischen Eigenschaften, im entsprechenden Unterkapitel des jeweiligen Betriebsmodells konkretisiert und ergänzt.

4.1.1 Dokumentation

Unabhängig von dem Betriebsmodell muss laut BWI-Anforderungen der Informationssicherheit (Vorgaben DEV.A3 und CON.8.A12) für den Betrieb ein InfoSichhK (siehe Kapitel Security & Compliance) sowie ein Betriebshandbuch erstellt werden.

- [MUSS]: Das Betriebshandbuch muss die folgenden Punkte beschreiben.
  - Kontakt zu den jeweiligen Ansprechpartnern.
  - Zugriffsmöglichkeiten auf das System und die unterliegende Infrastruktur.
  - Architekturübersicht nebst Schnittstellen zu Drittsystemen.
  - Anweisungen für Installation und Wiederanlauf.
  - Konfigurationsparameter.
  - Hinweise zu Wartung und zur Fehlerbehandlung.
  - Werkzeuge zur Administration.
  - Datensicherungs- und Wiederherstellungskonzept (Georedundante Aufbewahrung, Backup-Strategie, Backup-Medien, Restore: rechtliche Betrachtung).

4.1.2 Signierung

Bzgl. der Signierung von Artefakten ist folgendes zu beachten:

- [MUSS]: Alle Artefakte (z. B. der Code bzw. das ausgelieferte Modul/Container) sind zu signieren (siehe CON.8.A8 und Orientierungshilfe Informationssicherheitsanforderungen im Verweise auf andere Dokumente).

4.1.3 Deployment

Die Prozesse zur Installation von Software und Konfigurationen auf einen oder mehreren Rechnern (Umgebung) wird als Software Deployment (Softwareverteilung) bezeichnet. Der finale Schritt des (Continuous-)Deployments ist der "commercial launch" bzw. "go live".

Dabei gilt:

- [MUSS]: Es muss ersichtlich sein, welche Version der Software auf welcher Umgebung aktuell läuft.
- [MUSS]: Es muss ersichtlich sein, welche Version der Software in welchem Zeitraum gelaufen ist.
- [MUSS]: Es muss darauf geachtet werden, dass die Lauffähigkeit in der jeweiligen Umgebung gegeben ist, deshalb muss eine Abhängigkeitsmatrix gepflegt werden.
- [MUSS]: Das Software Deployment richtet sich nach den Gegebenheiten der Kundenumgebungen und eingesetzten Technologien.
- [EMPFOHLEN]: Während der Entwicklung soll ein Deployment in eine möglichst produktionsnahe Testumgebung erfolgen, um durch entsprechende Tests die Qualität und Realitätstreue zu sichern (siehe Kapitel Software Quality & Assurance).
- [EMPFOHLEN]: Das Software Deployment soll möglichst automatisiert ablaufen.

4.1.4 Inbetriebnahme

Bei initialem Produktionsdeployment sowie bei Major Updates gilt:

- [MUSS]: Für die Inbetriebnahme eines Anwendungssystems muss eine erhöhte Bereitschaft des Entwicklungsteams eingeplant werden.
  - [EMPFOHLEN]: Bereitschaft für das initiale Produktivsetzung: 8 Wochen.
  - [EMPFOHLEN]: Bereitschaft für Major Updates: 2 Wochen.

4.1.5 Operating

Mit dem Start des Deployments startet das Operating (Betrieb) und damit auch die Wartungsphase (siehe Kapitel Maintenance & Support). Nach dem Go-Live nutzen erste Kunden das neue Softwareprodukt. Standardmäßig ist der "End of Life"-Zustand für ein Produkt nach drei Jahren erreicht (Abweichungen sind möglich, müssen aber explizit dokumentiert werden).

Ausgelieferte Produkte sollen ein optimales Verhalten zur Laufzeit bieten. Dazu gehören neben den Aspekten des professionellen Application Managements:

- [MUSS]: Stabiler Neustart: Die Produkte werden so designt, dass zu jedem Zeitpunkt ein Neustart möglich ist ohne inkonsistente Zustände z. B. in Datenbanken zu hinterlassen.
- [MUSS]: Readiness: Die Produkte enthalten Schnittstellen, die eine Betriebsumgebung erkennen lassen, dass ein Produkt einsetzbar ist.
- [MUSS]: Health Checks / Liveness probe: Health Checks werden implementiert, damit das überwachende System den aktuellen Zustand eines Produktes bewerten kann und ggf. Maßnahmen ergreifen kann. Voraussetzung ist, dass das System so etwas zulässt.

4.1.6 Monitoring & Reporting

Die Überwachung einer Anwendung ist ebenso wichtig wie deren Entwicklung, damit eine optimale User Experience gewährleistet werden kann. Aus diesem Grund ist eine proaktive Überwachungsstrategie erforderlich. Fehler, Leistungsparameter, Verfügbarkeit und Ausfallzeiten müssen transparent für Entwicklung und Operation zugänglich sein. Die Tiefe des Application Performance Monitorings ist abhängig vom jeweiligen Geschäftsfall und muss im Rahmen des Projekts betrachtet und festgelegt werden. Das Monitoring muss immer gemäß der Vorgaben der Sicherheitsdomäne erfolgen.

Application Performance Monitoring

Drei Arten von APM Tools sind zu berücksichtigen:

- [EMPFOHLEN]: Anwendungsmetriken
- [EMPFOHLEN]: Code-Profiling
- [EMPFOHLEN]: Netzwerk

Es sollten alle drei Arten eingesetzt werden, um zur Laufzeit einen allumfassenden Blick in die Software zu bekommen.

Relevante Kriterien dabei sind:

- [EMPFOHLEN]: Performance der Anwendung
- [EMPFOHLEN]: Ressourcenverbrauch
- [EMPFOHLEN]: Stabilität
- [EMPFOHLEN]: Anonymisierte Benutzeraktivitäten

Diese Kriterien liefern in erster Linie einen Rückschluss auf den fehlerfreien Ablauf der Software sowie der Validierung der User Experience.

Reporting

Für das Reporting gilt:

- [MUSS]: Es muss gewährleistet werden, dass ein regelmäßiges Reporting über die Funktionsweise der Applikation bereitgestellt werden kann. Dies erfolgt z. B. über einen Health-Check-Report. Funktionale (Teil-)Ausfälle soll die Anwendung proaktiv reporten, z. B. über SIEM. Hierbei muss sich die Applikation in den Informationsverbund eingliedern, in dem sie betrieben wird.
- [MUSS]: Es muss gewährleistet werden, dass ein regelmäßiges Reporting über potenzielle Schwachstellen der Applikation bereitgestellt werden kann. Dies betrifft die Applikation ganzheitlich, d.h. die Komposition der Anwendung muss regelmäßig durch die Software-Komponentenanalyse verifiziert werden.
- [MUSS]: Die Vorgaben BSI CON.8.A6, BSI CON.8.A20, BSI OPS1.1.5, BWI InfSichhRiLi - Monitoring & Schwachstellen-Scans (siehe auch Kapitel Security & Compliance) sind einzuhalten.

4.2 Server-based Applications

Ansprechpartner: Holger Brinkmann, BWI

Dieses Kapitel dient gemeinsam mit den allgemeinen Operating Vorgaben aus Software-Engineering-Sicht als Leitfaden für das Betriebsmodell Server-based Applications in der BWI.

4.2.1 Deployment

Klassisches Application Hosting durch die BWI wird durch den Service 210 Application Hosting Server (AHS) (Kontakt: bwi.fp.ssd-sl-pf-sah@bwi.de) durchgeführt. Das Hosting ist grundsätzlich stark abhängig von den eingesetzten Technologien und dem Anwendungsfall. Daher gibt es aktuell kein allgemeingültiges Vorgehen für das Deployment. Stattdessen muss das Deployment mit den zuständigen Teams aus AHS für den konkreten Fall ausgearbeitet werden. Hierfür gelten die folgenden Vorgaben:

- [MUSS]: Frühzeitiges Einbeziehen von AHS mit Informationen über den Anwendungsfall und die Zielarchitektur, inkl. Klärung der aktuellen Anforderungen, Rahmenbedingungen und Verantwortlichkeiten. AHS liefert hier bereits ein Portfolio über Standards (z. B. zu Managed Server, Datenbanken, Middleware). Dieses Portfolio kann in Absprache mit AHS erweitert werden.
- [MUSS]: Festlegen eines Deployment-Prozesses in Abstimmung mit AHS, unter der Berücksichtigung der dort festgelegten Prozesse.
- [MUSS]: Übergabe des getesteten und lauffähigen Softwareartefakts an AHS.
- [MUSS]: Übergabe sowie Aktualisierung der von AHS geforderten Dokumentation. Dies umfasst in der Regel mindestens das InfoSichhK sowie das Betriebshandbuch.
- [EMPFOHLEN]: Einsatz eines Artefaktspeichers.

4.2.2 Operating

Wie beim Deployment handelt es sich auch beim Operating Modell um das klassische Application Hosting über den Service 210 AHS. Hier laufen die Fäden aller für den Betrieb einer Anwendung notwendigen Services (z. B. Managed Database, Managed Server) zusammen.

AHS koordiniert im Falle von Änderungen an den einzelnen Komponenten die einzelnen Prozessschritte basierend auf dem abgestimmten ITIL-Prozess. Der Bedarf für Änderungen an den Komponenten entsteht durch notwendige Software Updates, durch Wartungsintervalle oder auch durch den Kunden beauftragte Software-Pflege-Änderungsmaßnahmen (SWPÄ).

Folgende Aktivitäten sind zu berücksichtigen:

- [MUSS]: Erstellung eines SWPÄ-Konzeptes.
- [EMPFOHLEN]: Erstellung eines Konzeptes zur Außerbetriebnahme (in Kooperation mit dem Betrieb).

4.2.3 Monitoring & Reporting

siehe Allgemeine Operating Vorgaben.

Für eine vollständige End-to-End-Monitoring-Strategie sind folgende Aktivitäten zu beachten:

- [MUSS]: Backend-Fehler protokollieren.
- [MUSS]: Automatische Fehlerreports erstellen.
- [MUSS]: Automatische Alarmierung bei schwerwiegenden Fehlern.
- [MUSS]: Proaktive Erkennung von Sicherheitsproblemen durch Anbindung an Security Information and Event Management (SIEM).
- [EMPFOHLEN]: Performance-Probleme analysieren.
- [EMPFOHLEN]: User-Interaktionen anonymisiert erfassen.
- [EMPFOHLEN]: Router Changes / Page Transitions tracken (unter Beachtung geltender Compliance-Regeln).
- [EMPFOHLEN]: Erfassung von Metriken und Bereitstellung von Auswertetools.
- [EMPFOHLEN]: Dashboard Reports kontinuierlich überwachen.
- [EMPFOHLEN]: Tracing Frontend to Backend durch Korrelation von Loggings (Interservice-Kommunikation).
- [EMPFOHLEN]: Automatiken zur Lösung entwickeln.
- [EMPFOHLEN]: Um das Logging in verteilten System zentral zu sammeln, wird z. B. der ELK-Stack empfohlen (siehe Allgemeine Guideline, Abschnitt Logging).

4.3 Cloud Applications

Ansprechpartner: Burkhard Pietsch, BWI

Dieses Kapitel dient gemeinsam mit den allgemeinen Operating Vorgaben aus Software-Engineering-Sicht als Leitfaden für das Betriebsmodell Cloud Applications in der BWI.

4.3.1 Deployment

Zielumgebungen sind:

- pCloudBw
  Das Artefakt wird in einen Artefaktspeicher eingebracht und gemäß der pCloud Software-Deployment-Platform (SDP) und den Produktvorgaben ausgebracht.
- Andere private Clouds (bei Kundenanforderung)
  Das Artefakt wird in einen Artefaktspeicher eingebracht und gemäß den Produktvorgaben ausgebracht.
- Public Clouds (bei Kundenanforderung)
  Deployment nach den jeweiligen Gegebenheiten des Cloud-Providers.

Folgende Aktivitäten sind notwendig:

- [MUSS]: Releaseartefakte werden unveränderbar in einen geeigneten Artefaktspeicher abgelegt.
- [MUSS]: Die aktuelle (eindeutige) Version ist in der Umgebung ersichtlich.
- [MUSS]: Dokumentation enthält Informationen, wann welche Version der Software in welcher Umgebung läuft/ gelaufen ist.*
- [MUSS]: Alle Artefakte sind signiert.
- [MUSS]: Automatisiertes Deployment ist für alle angeforderten Umgebungen vorhanden.*
  * Kann nur unter DevOps Bedingungen von dem Entwicklungsteam erfüllt werden.

4.3.2 Operating

siehe Allgemeine Operating Vorgaben.

4.3.3 Monitoring & Reporting

siehe Allgemeine Operating Vorgaben.

Für eine vollständige End-to-End Monitoring Strategie sind folgende Aktivitäten notwendig:

- [MUSS]: Backend-Fehler protokollieren.
- [MUSS]: Automatische Fehlerreports erstellen.
- [MUSS]: Automatische Alarmierung bei schwerwiegenden Fehlern.
- [MUSS]: Proaktive Erkennung von Sicherheitsproblemen durch Anbindung an Security Information and Event Management (SIEM).

- [EMPFOHLEN]: Performance-Probleme analysieren.
- [EMPFOHLEN]: User-Interaktionen anonymisiert erfassen.
- [EMPFOHLEN]: Router Changes / Page Transitions tracken (unter Beachtung geltender Compliance-Regeln).
- [EMPFOHLEN]: Erfassung von Metriken und Bereitstellung von Auswertetools.
- [EMPFOHLEN]: Dashboard Reports kontinuierlich überwachen.
- [EMPFOHLEN]: Tracing Frontend to Backend durch Korrelation von Loggings (Interservice-Kommunikation).
- [EMPFOHLEN]: Automatiken zur Lösung entwickeln.
- [EMPFOHLEN]: Um das Logging in verteilten System zentral zu sammeln, wird z. B. der ELK-Stack empfohlen (siehe Allgemeine Guideline, Abschnitt Logging).

4.4 Desktop Applications

Ansprechpartner: Günter Liehl, BWI

Dieses Kapitel dient aus Software-Engineering-Sicht als Leitfaden für das Betriebsmodell Desktop Applications in der BWI. Grundsätzlich sind ebenfalls die allgemeinen Operating Vorgaben zu berücksichtigen, sofern diese im Kontext Desktop Applications anwendbar sind.

4.4.1 Deployment

Die Applikation wird zur Paketierung/Verteilung an SSD Point of Delivery 1 Workplace Software Management (Kontakt: bwi.fp.ssd-sl-dw-swm-standardsoftware@bwi.de) übergeben, die Verteilung erfolgt via SCCM.

- [MUSS]: Die Windows-Anwendung muss als installierbares .msi file ausgeliefert werden mit folgenden Eigenschaften:
  - Unattended Installation ohne Benutzerinteraktion.
  - msi Installation erledigt wirklich nur die Installation, keine Konfiguration der Anwendung (Ablage generell in "Program Files").
  - Konfigurationsdaten per .config file (bevorzugt), alternativ Registry.
  - Installation per Machine (per User nur dann, wenn z. B. per User-Lizenzen fällig sind).
  - Updates per follow up msi (Aktualisierung der bestehenden Installation durch die Ausführung des neuen Installationspaketes) - Upgrade-Codes beachten.
  - Öffnungen der lokalen Windows-Firewall durch den Installer müssen genehmigt werden.
  - De-Installation muss die Anwendung komplett entfernen (incl. Benutzerspezifischen .config-Daten, Registry Einträge, etc. - hier auch ggf. geänderte Firewall-Regeln wiederherstellen!).
  - MSIs müssen signiert sein, ebenso alle Komponenten im MSI die sinnvoll signiert werden können (.dll, .exe, ps1 scripte, etc.).
    Hinweis: 3rd Party Komponenten (z. B. dll-Dateien) behalten die Signatur vom Hersteller, sollte der Hersteller keine Signierung vornehmen, wird die dll mit unserem Zertifikat nachsigniert (muss dokumentiert werden!).

Die Deployment-, Staging- und Abnahmetests der Anwendung müssen auf einem produktionsnahen Endgerät (APC) stattfinden. Ein Testgerät kann bei SSD Point of Delivery 1 Workplace Software Management angefragt werden.

Links zu SSD Point of Delivery 1 Workplace Software Management zum nachlesen: Paketierungsrichtlinie und Paketierungsstrategie.

4.4.2 Operating

- Der Betrieb einer Desktop Applikation beginnt mit der Übergabe und Verteilung der Applikation an die Clients.
- Die Verantwortung liegt dann bei SSD Point of Delivery 1 Workplace Software Management .

4.4.3 Monitoring & Reporting

- Logging in das NT Event-Log (typischerweise Applikationsspezifische Log Senke).
- Tracing in eine Logdatei (log Rotation, Größe beachten).
- HealthCheck/Lifeliness Schnittstelle:
  - Service-behaftete Anwendungen (also Anwendungen die immer ausgeführt werden) müssen eine HealthCheck/Lifeliness-Schnittstelle im Service Control Interface implementieren, damit die ordnungsgemäße Ausführung des Services (auch remote) überprüft werden kann.
  - Beinhaltet der Service z. B. eine Kommunikationsschnittstelle sollte ein Performance Counter implementiert werden um den Datendurchsatz monitoren zu können.

Für eine vollständige End-to-End Monitoring Strategie sind folgende Aktivitäten notwendig:

- [MUSS]: Frontend-Fehler protokollieren.
- [MUSS]: Netzwerkfehler protokollieren.
- [MUSS]: Backendfehler protokollieren.
- [MUSS]: Automatische Fehlerreports erstellen.
- [MUSS]: Automatische Alarmierung bei schwerwiegenden Fehlern in Backend oder Frontend.
- [EMPFOHLEN]: Performance Probleme analysieren.
- [EMPFOHLEN]: User Interaktionen anonymisiert erfassen.
- [EMPFOHLEN]: Alarme werden an SPOC geliefert.
- [EMPFOHLEN]: Interservice Kommunikation monitoren.
- [EMPFOHLEN]: Proaktive Erkennung von Sicherheitsproblemen durch Security Information and Event Management (SIEM).
- [EMPFOHLEN]: Automatiken zur Lösung entwickeln.

4.5 Mobile Applications

Ansprechpartner: Jürgen Wischer, BWI

Dieses Kapitel dient aus Software-Engineering-Sicht als Leitfaden für das Betriebsmodell Mobile Applications in der BWI. Grundsätzlich sind ebenfalls die allgemeinen Operating Vorgaben zu berücksichtigen, sofern diese im Kontext Mobile Applications anwendbar sind.

Informationen zur Entwicklung von Apps sind in den Kapiteln Swift und Kotlin zu finden.

4.5.1 Signierung

Android

- [MUSS]: Pro App muss ein separates Zertifikat generiert werden. Neue Zertifikate lassen sich über das Android Studio erzeugen.
- [EMPFOHLEN]: Bei Verteilung der App über den Play Store sollte das Google Play Signing verwendet werden.

iOS

- [MUSS]: iOS Apps verwenden immer das von Apple standardisierte App Signing Verfahren.

4.5.2 Deployment

In der BWI werden mobile Applikation auf zwei Arten veröffentlicht: über den Play-/App Store oder über ein Mobile Device Management (MDM).

- [MUSS]: Es muss eine geeignete Art zur Veröffentlichung gewählt werden. Bei privaten Geräten ist die Veröffentlichung über einen öffentlichen App Store zu wählen.
- [MUSS]: Es muss eine öffentliche Datenschutzerklärung bereitgestellt werden. Innerhalb der BWI kann die Unternehmenskommunikation bei der Veröffentlichung unterstützen (Kontakt: bwi.fp.comm-kanaele@bwi.de).
- [MUSS]: Innerhalb der BWI muss die Unternehmenskommunikation bei der Erstellung der App-Store-Inhalte (Grafiken, textuelle Beschreibungen) eingebunden werden.
- [EMPFOHLEN]: Wenn möglich sollten alle Apps über die Stores veröffentlicht werden. Diese können sowohl komplett öffentlich oder nur intern für bestimmte Organisationen (z. B. BWI oder Bw) bereitgestellt werden.
- [EMPFOHLEN]: Die Apps sollten vor Veröffentlichung durch einen PEN Test geprüft werden. Innerhalb der BWI kann hier auf die Abteilung CDO CCITS CERT/SOC Operation zugegangen werden.
- [KANN]: Bei dienstlichen Geräten besteht zusätzlich die Möglichkeit zur Veröffentlichung über MDM.

Veröffentlichung von öffentlichen Apps über die App Stores

- [MUSS]: Die entsprechenden Guidelines für die Veröffentlichung von Apps in den Stores von Google & Apple sind zu beachten:

- Android:
  - https://developer.android.com/studio/publish
  - https://play.google.com/about/developer-content-policy/
- iOS
  - https://developer.apple.com/app-store/review/guidelines/

- [MUSS]: Vor der Veröffentlichung und der Länderauswahl muss geprüft werden, ob Exportkontrollrechte zum Einsatz kommen und ggf. zu beachten sind. Insbesondere der Einsatz von Crypto-Bibliotheken ist kritisch. Weitere Infos dazu hier:
  - Complying with Encryption Export Regulations | Apple Developer Documentation
  - Export compliance - Play Console Help (google.com)

- [EMPFOHLEN]: Für die Bereitstellung von Beta Apps oder für interne Testzwecke eignen sich die bereits vorhandenen Lösungen in den App Stores (Apple Testflight & Test Tracks).
- [EMPFOHLEN]: Nutzung von gestaffelten Releases zur frühzeitigen Kontrolle von Problemen mit den Apps.

Veröffentlichung von internen Apps über die App Stores

- [MUSS]: Die entsprechenden Guidelines für die Veröffentlichung von Apps in den Stores von Google & Apple sind zu beachten:
  - Android
    - https://developer.android.com/studio/publish
    - https://play.google.com/about/developer-content-policy/
  - iOS
    - https://developer.apple.com/app-store/review/guidelines/
- [MUSS]: Die Konfiguration für interne / private Apps muss entsprechend durchgeführt werden. Die korrespondierenden Ids können über den Service Enterprise Mobility Management (Kontakt: bwi.fp.SSD-SL-CM-EMM@bwi.de) angefragt werden.
  - Android: Interne Apps bereitstellen - Managed Play Store-Hilfe (google.com)
  - iOS: Set your app's distribution methods - App Store Connect Help (apple.com)
- [MUSS]: Für die weitere Verteilung von Apps über MDM muss das Enterprise Mobility Management (Kontakt: bwi.fp.SSD-SL-CM-EMM@bwi.de) eingebunden werden.
- [EMPFOHLEN]: Für die Bereitstellung von Beta Apps oder für interne Testzwecke eignen sich die bereits vorhandenen Lösungen in den App Stores (Apple Testflight & Test Tracks).
- [EMPFOHLEN]: Nutzung von gestaffelten Releases zur frühzeitigen Kontrolle von Problemen mit den Apps.

Verteilung per MDM über private App Stores (VS-NfD Apps)

- [MUSS]: Für die Bereitstellung und Härtung von VS-NfD-Apps muss das Enterprise Mobility Management (Kontakt: bwi.fp.SSD-SL-CM-EMM@bwi.de) eingebunden werden.
- [EMPFOHLEN]: Es muss ein Vorlauf von mind. 6-9 Monaten eingeplant werden, da die Apps i.d.R. noch durch SecuSmart und BSI geprüft werden.

4.5.3 Operating

Der Betrieb von mobilen Applikationen beginnt mit der Bereitstellung über die entsprechenden App Stores oder über das Mobile Device Management.

4.5.4 Monitoring & Reporting

Die Möglichkeiten der App-Analyse sind eingeschränkt und weitestgehend auf die Werkzeuge der Hersteller Google bzw. Apple zu beschränken. Diese sollen so umfassend wie möglich genutzt werden. Das umfassende Performance Monitoring aus den allgemeinen Vorgaben kann daher nur auf Testgeräten durchgeführt werden. Im Folgenden werden die Analysen aufgeführt, die zur Laufzeit auf den Endgeräten der Nutzer*innen erfasst werden können.

Absturzanalyse

- [MUSS]: Die Nutzung der integrierten Analysetools der einzelnen Plattformen ist für die über die App Stores veröffentliche Apps verpflichtend.
- [EMPFOHLEN]: Für neu gemeldete Abstürze sollen Intervalle festgelegt werden, innerhalb derer das Team die Abstürze überprüft und bewertet.
- [KANN]: Absturzdaten von Beta- und Testversionen können ebenfalls auf die zuvor genannte Art behandelt werden.
- [KANN]: Der Einsatz von App Obfuscation ist optional bzw. abhängig von den Sicherheitsanforderungen der App. Falls Obfuscation eingesetzt wird, müssen Best Practices zum Einsatz entsprechender Tools und zur Auflösung der obfuskierten Absturzlogs etabliert werden.

App-Analyse

- [MUSS]: Die Nutzung von cloudbasierten Analysetools (z. B. Google Analytics) ist auszuschalten.
- [EMPFOHLEN]: Bei Verteilung über öffentliche App Stores sollten die allgemeinen Daten genutzt und analysiert werden z. B.:
  - Verbreitung der OS Version.
  - Updateverhalten der Nutzer*innen.
  - Download & Nutzungszahlen.
  - Abstürze.
- [KANN]: Nutzung von On-Premise-Lösungen (z. B. Matomo über Service Web Analytics) sind möglich, müssen aber mit dem Kunden / AG abgesprochen werden. Hierbei muss der Datenschutz beachtet werden. Aus den Analysedaten darf kein Verhalten der einzelnen Nutzer*innen abgeleitet werden können.

Rezensionen in den App Stores

- [MUSS]: Rezensionen müssen regelmäßig überprüft, gelesen und beantwortet werden.
- [EMPFOHLEN]: Auffälligkeiten in den Rezensionen (Fehler & Feature Wünsche) sollten in die Entwicklung einfließen.

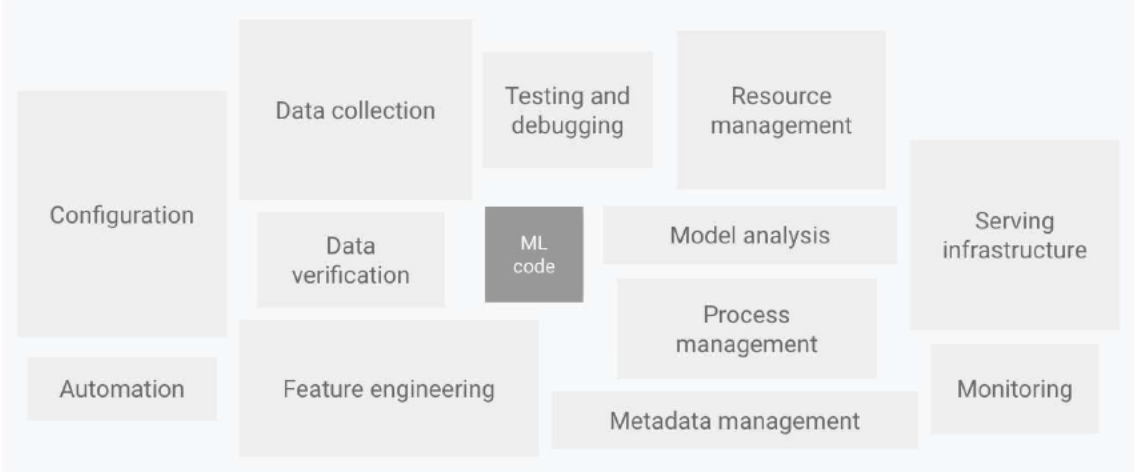
4.6 AI Applications

Ansprechpartner: Dr. Fabian Köhlinger, BWI; Dr. Jan Strohschein, BWI; Pierre Rosengaft, BWI

Sämtliche Inhalte in diesem Kapitel basieren auf: MLOps: Continuous Delivery und Pipelines zur Automatisierung im maschinellen Lernen. Einige grundlegende Definitionen von zentralen MLOps-Begriffen/Bestandteilen befinden sich im Glossar .

Das Konzept von Machine Learning Operations (MLOps) verwendet viele bekannte DevOps-Ansätze wieder, sowohl bei der Entwicklung als auch beim Betrieb von Machine Learning (ML)-Anwendungen und/oder Anwendungen, die künstliche Intelligenz (KI) verwenden. Dabei bestehen jedoch einige zentrale Unterschiede zu herkömmlichen Softwareprojekten, die ein erweitertes Konzept rechtfertigen. Für tiefergehende Details zu diesem Konzept empfehlen wir auch: DevOps im Vergleich zu MLOps.

Zur Verdeutlichung der Komplexität von modernen ML-Systemen wird in der gängigen Literatur gerne die folgende Grafik referenziert, die verdeutlicht, dass der eigentliche ML-Code / ML-Algorithmus nur der kleinste Teil in einem ML-System (in Produktion) ist und ein erweitertes Konzept zur Entwicklung und Betrieb eines solchen Systems rechtfertigt:



Quelle: Elemente für ML-Systeme (Google)

4.6.1 Vorgaben zu MLOps-Reifegradmodellen

Basierend auf den typischen Komponenten des MLOps-Lifecycles (siehe Glossar) wird weiterhin zwischen verschiedenen MLOps-Reifegradmodellen unterschieden. Anschaulich fängt der niedrigste Grad beim typischen Skripten mit (z. B. Jupyter) Notebooks an und kann dann in den höheren Graden eine Komplexität von automatisierten MLOps-Pipelines erreichen, die als Antwort auf eine kontinuierliche Überwachung der ML-Modell-Performance ein erneutes Training des gesamtem ML-Modells durchführen und auch direkt in Produktion deployen.

Basierend auf den Best-Practices der großen (Public) Cloud-Anbieter wie z. B. AWS, Microsoft oder Google, führen wir im Nachgang die bewährten drei Reifegradmodelle ein, beschreiben diese kurz und leiten Handlungsempfehlungen ab.

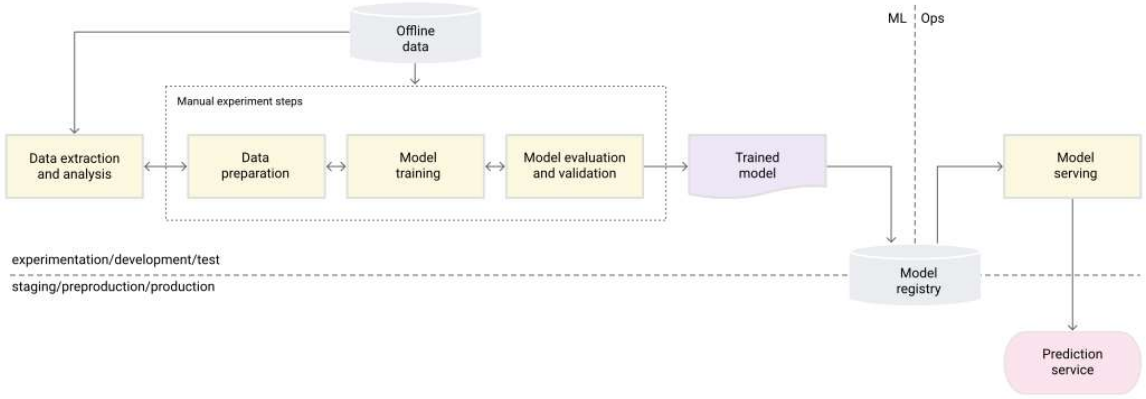
Die Handlungsempfehlungen beziehen sich hierbei auf folgende Zielumgebungen:

- pCloudBw
  MLOps muss mit den Tools der Data Analytics Platform (DAP) gemäß der jeweils für das Projekt passenden Reifegradstufe erfolgen (für Produktion mind. Stufe 1).

- Andere private Clouds bei Kundenanforderung
  MLOps muss mit den Tools der DAP oder auf der Plattform bereits bereitgestellten Tech-Stack gemäß der jeweils für das Projekt passenden Reifegradstufe erfolgen (für Produktion mind. Stufe 1).
- Public Clouds bei Kundenanforderung
  MLOps nach den jeweiligen Gegebenheiten des Cloud-Providers.

MLOps-Stufe 0: Manueller Prozess (nur für PoC vorgesehen)

In der einfachen Reifestufe oder Stufe 0 erfolgt der Prozess zum Erstellen und Bereitstellen von ML-Modellen vollständig manuell. Typisch für diese Stufe ist eine kleine, manuell verwaltete Anzahl von Modellen mit seltenen Updates (wenige Male pro Jahr). Das folgende Diagramm zeigt den typischen Workflow des Prozesses:



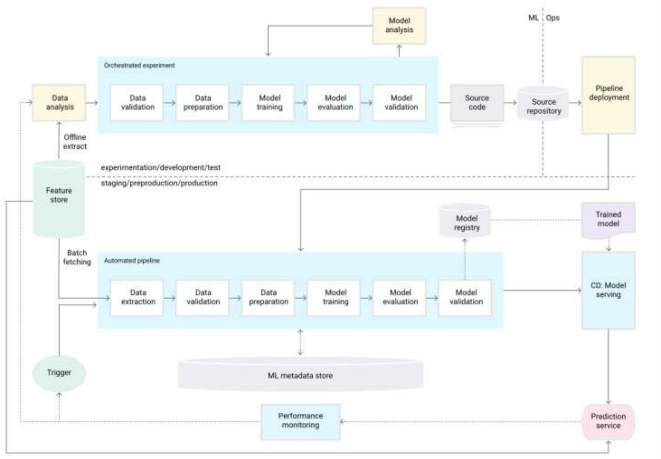
Quelle: [Manuelle ML-Schritte zur Bereitstellung des Modells als Vorhersagedienst (Google)]

Aus diesem Workflow leiten sich die folgenden Vorgaben ab:

- [MUSS]: Modellentwicklung erfolgt in versionskontrolliertem Notebook oder Skript.
- [MUSS]: Testen des Codes / des Modells findet in Notebooks / Skripts statt.
- [MUSS]: Bereitstellung (z. B. per REST-API) bezieht sich nur auf das Modell selbst.
- [MUSS]: (mind. manuelles) Testing bevor das Modell / aktualisierte Version des Modells bereitgestellt wird (z. B. per REST-API).
- [EMPFOHLEN]: Model-Monitoring zur Erkennung von Performance-Einbußen und von veralteten Modellen.
- [EMPFOHLEN]: Regelmäßiges Neu-trainieren der Modelle mit aktualisierten Daten.
- [EMPFOHLEN]: Modellentwicklung sollte in Python mit entsprechenden Frameworks (z. B. scikit-learn, TensorFlow, PyTorch) erfolgen.
- [EMPFOHLEN]: Fertig trainiertes Modell wird in Model Registry hochgeladen.
- [EMPFOHLEN]: Fortlaufendes (manuelles) Experimentieren mit neuen Implementierungen (z. B. Feature Engineering, Modellarchitektur, Hyperparameter) bei der Erstellung des Modells.

MLOps-Stufe 1: ML-Pipelineautomatisierung

Ziel dieser Stufe ist es, durch Automatisierung der ML-Pipeline ein kontinuierliches Training des Modells zu ermöglichen. Zugleich wird so die kontinuierliche Bereitstellung des Modellvorhersagedienstes erreicht. Zur Automatisierung des Prozesses, bei dem neue Daten zum erneuten Trainieren von Modellen in der Produktion verwendet werden, müssen in der Pipeline automatisierte Daten- und Modellvalidierungsschritte sowie Pipeline-Trigger und die Metadatenverwaltung eingeführt werden. Das folgende Diagramm zeigt den typischen Workflow dieses Prozesses:



Quelle: [ML-Pipelineautomatisierung für CT (Google)]

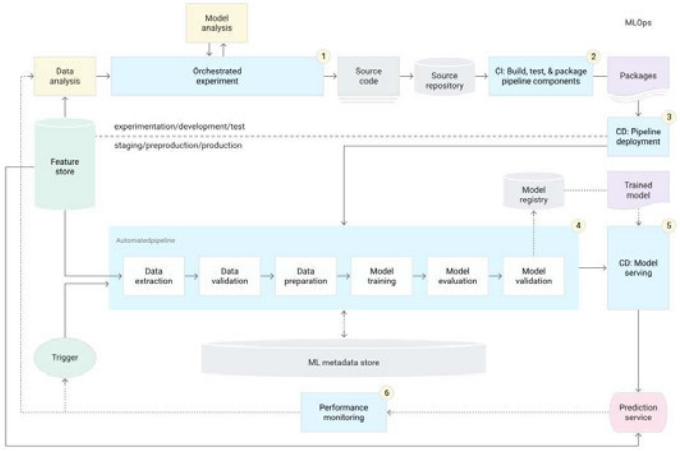
Aus diesem Workflow leiten sich die folgenden Vorgaben ab:

- [MUSS]: Automatisierte Datenvalidierung erkennt Anomalien von Datenschematas oder -werten.
- [MUSS]: Automatisierte Modellvalidierung erstellt Bewertungsmesswerte mithilfe eines Test-Datasets.
- [MUSS]: Pipelines für automatisiertes Modelltraining und -deployment.
- [MUSS]: Model-Monitoring zur Erkennung von Performance-Einbußen und von veralteten Modellen.
- [MUSS]: Pipeline Trigger (manuell, Intervall, ereignisbasiert, z. B. neue Daten, Model-Performance, Concept-Drift).
- [MUSS]: Automatisiertes Testing bevor das Modell / aktualisierte Version des Modells bereitgestellt wird (z. B. per REST-API).
- [MUSS]: Vereinheitlichung der Pipelineimplementierung über die verschiedenen Umgebungen.
- [MUSS]: Modularisierter Komponentencode für Wiederverwendbarkeit und Kompositionsmöglichkeiten.
- [MUSS]: Komponenten werden containerisiert.
- [MUSS]: Fertig trainiertes Modell wird in Model Registry hochgeladen.
- [MUSS]: Metadatenverwaltung zeichnet Herkunft von Daten und Artefakten zu einzelnen Ausführungen der ML-Pipeline auf und ermöglicht damit eine Reproduzierbarkeit und Vergleichbarkeit.

- [EMPFOHLEN]: Feature Store als zentrales Repository für Definition, Speicherung und Zugriff auf Features.

MLOps-Stufe 2: CI/CD-Pipelineautomatisierung

Zusammengefasst beinhaltet die Implementierung von ML in einer Produktionsumgebung in der Stufe 2 nicht nur die Bereitstellung des ML-Modells als API für Vorhersagen. Die Implementierung umfasst vielmehr die Bereitstellung einer ML-Pipeline, mit der das erneute Trainieren und Bereitstellen neuer Modelle automatisiert werden kann. Durch die Einrichtung eines CI/CD-Systems können neue Pipelineimplementierungen automatisch getestet und bereitgestellt werden. Mithilfe dieses Systems kann souverän auf rasche Veränderungen der Daten und der Unternehmensumgebung reagiert werden. Der Reifegrad 2 sollte das Zielbild für große und langlaufende Projekte sein, um die Erweiterbarkeit und Wartbarkeit des Systems gewährleisten zu können. Das folgende Diagramm zeigt den typischen Workflow dieses Prozesses:



Quelle: [CI/CD und automatisierte ML-Pipeline (Google)]

Aus diesem Workflow leiten sich zusätzlich zu den Kriterien aus Stufe 1 die folgenden Vorgaben ab:

- [MUSS]: Quellcode von ML-Pipelineschritten muss versionskontrolliert in ein Quell-Repository übertragen werden (Reproduzierbarkeit).
- [MUSS]: Pipelinekomponenten (Pakete, ausführbare Dateien und Artefakte) werden per Continuous Integration (CI) aus getestetem und versionskontrolliertem Quellcode heraus bereitgestellt.
- [MUSS]: Die in der CI-Phase erzeugten Artefakte werden durch Continuous Deployment (CD) in der Zielumgebung in der jeweils neusten Implementierung des Modells ausgebracht.
- [MUSS]: Unit-Tests der verschiedenen im Modell implementierten Methoden in der CI.
- [MUSS]: Testen, dass Pipeline-Komponenten in der CI die erwarteten Artefakte erzeugen.
- [MUSS]: Integration-Tests für die Pipeline-Komponenten in der CI.
- [MUSS]: Tests für Model-Serving in der CD (besonders nach Aktualisierung des Modells).
- [MUSS]: Lasttests für Model-Serving in der CD (z. B.: Abfragen pro Sekunde, Modelllatenz).

- [MUSS]: Datenvalidierung in der CD sowohl für Re-Training als auch (Batch)Vorhersagen.
- [MUSS]: Test auf Konvergenz des Modelltrainings in der CI.
- [EMPFOHLEN]: Automatisierte Bereitstellung per CD in Vorproduktionsumgebung (z. B. nach einem Merge-Request mit erfolgreicher Peer-Review auf den Main-Branch).
- [EMPFOHLEN]: Unit-Tests der Feature-Engineering-Logik in der CI.
- [EMPFOHLEN]: Automatisierte Bereitstellung per CD in Testumgebung (z. B. ausgelöst durch Push auf Dev/Feature-Branch).
- [EMPFOHLEN]: Manuelle Bereitstellung in Produktion nach mehreren erfolgreichen Ausführungen der Pipeline in der Vorproduktionsumgebung.

4.7 Maintenance & Support

Ansprechpartner: Holger Brinkmann, BWI; Marcel Haßlinger, BWI

Das Thema Maintenance & Support ist für moderne, effiziente Softwareentwicklung essentiell und stärkt die Architekturprinzipen der BWI AP01 Adäquatheit und AP09 Robustheit. Die Verantwortung für ein Softwareprodukt geht über die Übergabe an den Kunden oder die Produktivsetzung hinaus. Ein Softwareprodukt benötigt über den gesamten Lebenszyklus hinweg Maintenance und Support, bis hin zur Ausphasung bzw. Retirement (End of Life). Generell gilt:

- [MUSS]: Unterstützen der Softwareprodukte zu jedem Zeitpunkt des Software-Lebenszyklus.

4.7.1 Support

Der Support für ein Softwareprodukt beginnt mit seiner Auslieferung und hat das Ziel, Nutzer und Betreiber zu befähigen, das System nutzen bzw. betreiben zu können. Dazu gehören die Fehlerbehebung im Fehlerfall, ggf. Installationshilfe und die grundlegende Unterstützung bei der Nutzung.

Dabei gilt:

- [MUSS]: Bereitstellung einer ausführlichen Dokumentation, zum Beispiel in Form eines Betriebshandbuchs (siehe Kapitel Allgemeine Operating Vorgaben).
- [MUSS]: Befähigen des 1st und 2nd Level Support zur Problemlösung durch eine vorbereitete Wissensdatenbank zu einem Softwareprodukt.
- [EMPFOHLEN]: Liefern einer abgestimmten Benutzerdokumentation passend zur Inbetriebnahme des Softwareprodukts.
- [KANN]: Unterstützen der Schulungsabteilung und deren Ausführenden bei der Erstellung von geeigneten Schulungsunterlagen (siehe Unterkapitel Schulungen).

4.7.2 Maintenance / Wartung

Die Wartung einer Software ist ein Teil des Software Supports. Sie beinhaltet korrigierende, präventive und optimierende Maßnahmen mit dem Ziel detektierte Fehler (z. B. aus dem Monitoring & Reporting oder durch Nutzer gemeldete) zu analysieren und zu beheben, Performanz oder andere Attribute zu verbessern oder Anpassungen an die veränderte Umgebung vorzunehmen. Dabei gilt:

- [MUSS]: Arbeiten an der kontinuierlichen Fehlerbehebung und Weiterentwicklung des Softwareprodukts im Auftrag des Kunden.
- [MUSS]: Durch geeignetes Monitoring und andere vorbeugende Maßnahmen Probleme frühzeitig erkennen und beheben.
- [KANN]: Unterstützung des Betriebs des Softwareprodukts auch nach der Inbetriebnahme durch das Projektteam.

4.7.3 Last-Level-Support

Der Last-Level-Support zielt darauf ab, schnellstmögliche Lösungen für Störungen zu finden, die höchstwahrscheinlich nur im Last-Level-Support gelöst werden können. Er gibt konkrete Handlungsanweisungen für alle Nutzer des Last-Level-Supports vor.

Die gängigen Fachbegriffe zu diesem Thema sind Problem und Incident.

- Ein Problem ist die Ursache für einen oder mehrere Incidents.
- Ein Incident ist eine ungeplante Unterbrechung oder Qualitätsminderung eines IT-Services bzw. ein Ereignis, das in der Zukunft einen IT-Service beeinträchtigen könnte.

Im Folgenden werden Incidents und Problems unter dem Begriff Störung zusammengefasst.

4.7.3.1 Proaktiver Last-Level-Support

- [EMPFOHLEN]: Implementierung von (self-healing) Mechanismen bzw. Automatismen, die die Funktionalität überprüfen und im Störungsfall automatisch erste Schritte durchführen. Dies können zum Beispiel ein Neustart und die Generierung eines Monitoring-Alarms sein. Insbesondere Standard-Fehler-Szenarien sollten proaktiv abgefangen werden, so dass die Nutzenden von einer guten User Experience profitieren und die Software uneingeschränkt verwenden können.

4.7.3.2 Prozess

In den nachfolgenden Abschnitten wird der Prozess zur Bearbeitung einer Störung beschrieben. Dabei orientiert er sich an nachfolgenden in der BWI gültigen Prozessen und Arbeitsanweisungen:

- Prozess ARIS - Problem- und Fehlerbehandlung durchführen
- Arbeitsanweisung ARIS - Problem Manager und Problem Supporter
- Arbeitsanweisung Beschreibung - Problem Manager und Problem Supporter

Störungen, die weder im 1st- noch 2nd-Level-Support gelöst werden können, werden an den Last-Level-Support weitergeleitet. Ausgewählte Personen aus dem Last-Level fungieren als Screener . Sie führen eine erste Sichtung durch und weisen die Störung an ein zuständiges Team oder einzelnen Entwickler weiter. Dabei gilt:

- [MUSS]: Störungen werden in einem Ticketsystem erfasst und gemanaged.
- [MUSS]: Das Ticket im Ticketsystem ist die "Single Source of Truth", auch wenn im Verlauf des Bearbeitungsprozesses weitere Aufgaben entstehen.
- [MUSS]: Das Ticket enthält immer alle relevanten Informationen über den Zustand und Status der Störung.
- [KANN]: Erfassung von relevanten Metriken zur Auswertung der Störungen im Last-Level-Support, sowie deren Bearbeitungszeit.

Bewertung und Klassifizierung

- [MUSS]: Inhaltliche Bewertung auf Vollständigkeit und Verständlichkeit.
- [MUSS]: Einstufung der Priorisierung (siehe Fehlerpriorität und Fehlerklassen im Kapitel Quality & Assurance).

- [EMPFOHLEN]: Ggf. Erfassung weiterer relevanter Informationen:
  - Zeitliche Informationen:
    Ab wann begann die Störung?
    Wann wurde die Störung bemerkt?
  - Welche Symptome treten auf?
  - Tritt die Störung regelmäßig oder unregelmäßig auf?
  - Durch wen wurde die Störung gemeldet?
  - Umgebung / Lokalisierungsfragen: Produkt / API / System
    Welche(s) System(e) sind betroffen?
    Welche Version des Systems ist betroffen?
  - Schritte zur Reproduktion der Störung, falls möglich.
  - Hilfreiche Artefakte, z. B. Log-Messages oder Screenshots.

- [MUSS]: Formale Bewertung:
  - Es handelt sich um keine Störung.
    - Ticket zurückweisen und Informierung des Störungsmelders mit Begründung.
  - Störung fällt in einen anderen Störungsbereich.
    - Zuständigkeit ermitteln und zuweisen.
    - Weiterleitung des Tickets an die passende Bearbeitergruppe.
  - Störung wird akzeptiert (siehe nächster Abschnitt).
    - Störung wird anhand der Prioritätseinstufung einem Entwicklungsprozess zugeordnet (Hotfix oder Regelbetrieb).

Störung wird akzeptiert

Wird die Störung akzeptiert, sind die folgenden fünf Schritte durchzuführen:

1. Ursachenforschung

- [MUSS]: Dazu sollen möglichst alle korrespondierenden Informationen gesammelt werden, um einen besseren Überblick über die Störung im Gesamtkontext zu erhalten. Hierzu sind insbesondere Logdateien auszuwerten und ein Betriebshandbuch zu Hilfe zu nehmen.
- [KANN]: Die Ursachenanalyse kann mit der Unterstützung durch Dritte erfolgen. Das können zum Beispiel weitere Teams oder andere Partner sein. Bei der Zusammenarbeit mit Dritten müssen die Richtlinien zur „Weitergabe von Protokolldaten und Speicherauszügen“ sowie ggf. „Fernwartung“ beachtet werden. Sofern diese Anforderungen eingehalten werden, und auch die vertraglichen Regelungen (NDA) in Ordnung sind, ist keine weitere Freigabe seitens CISO notwendig (vgl. Informationssicherheitsanforderungen).
- [EMPFOHLEN]: Hierzu können folgende Fragen herangezogen werden:
  - Durch welche Symptome äußert sich die Störung?
    - Existiert eine Störungsmeldung auf den Service-Dashboards (Metriken, Status, Auslastung, Quota, Uptime-Historie)?

- Auf welche Art schlägt das System fehl? Handelt es sich z. B. um eine Schleife, eine Blockierung, einen Absturz, um Leistungseinbußen oder um ein falsches Ergebnis?
- Sind externe Schnittstellen betroffen? Ggf. Zuhilfenahme von Verantwortlichen der entsprechenden Schnittstelle.
- Handelt es sich um eine schwerwiegende Störung? (Ist die gesamte Applikation betroffen oder nur teilweise? Wie groß ist der Anteil der betroffenen Nutzer?)

- Wo tritt die Störung auf?
  - Wie lauten die Fehlercodes und -nachrichten?
  - Betrifft die Störung nur ein Betriebssystem oder tritt es betriebssystemübergreifend auf?
  - Tritt die Störung in einer wohldefinierten technisch unterstützten Zielumgebung auf, d. h. wird die vom Nutzer gemeldete Störung in einer Umgebung oder Konfiguration genutzt, die von der Software-Entwicklung offiziell unterstützt wird? Sind z. B. technische Mindestanforderungen erfüllt?
  - Sind mehrere Anwender*innen / Systeme betroffen?
- Wann tritt die Störung auf?
  - Tritt die Störung regelmäßig oder unregelmäßig auf?
  - Trat die Störung bereits zuvor auf und wurde als gelöst gekennzeichnet (Wiederholungsstörung)?
  - Wie häufig tritt die Störung auf?
  - Welche Abfolge von Ereignissen geht der berichteten Störung unmittelbar voraus?
  - Tritt die Störung nach einer Änderung der Umgebung auf, wie beispielsweise nach einem Upgrade oder einer Installation von Hardware oder Software (Change Failure Rate)?
- Unter welchen Bedingungen tritt die Störung auf?
  - Besteht die Störung auch in der Vorgängerversion?
  - Treten zum selben Zeitpunkt auch andere Störungen auf?
- Kann die Störung reproduziert werden?
  - Wie lässt sich die Störung reproduzieren?
  - Lässt sich die Störung auch in der Integrations- und Testumgebung nachstellen?

2. Notwendigkeit eines Workarounds prüfen

- [MUSS]: Es muss geprüft werden, ob ein Workaround notwendig ist. Dabei sind folgende Ergebnisse und Aktivitäten möglich:
  - Workaround wird nicht benötigt.
  - Workaround wird benötigt und ist vorhanden.
    - Dokumentation in der Known Error Database und Kommunikation des Workarounds.
  - Workaround wird benötigt und ist nicht vorhanden.
    - Workaround entwickeln und verifizieren, sofern der Aufwand zur Erstellung eines Workarounds und die Auswirkung der Störung die Entwicklung rechtfertigen.
    - Es wird nach einer temporären Lösung bzw. einer Umgehungsmöglichkeit gesucht, die dem Incident Management bereit gestellt werden kann.
    - Dokumentation in der Known Error Database und Kommunikation des Workarounds.

3. Entwicklung

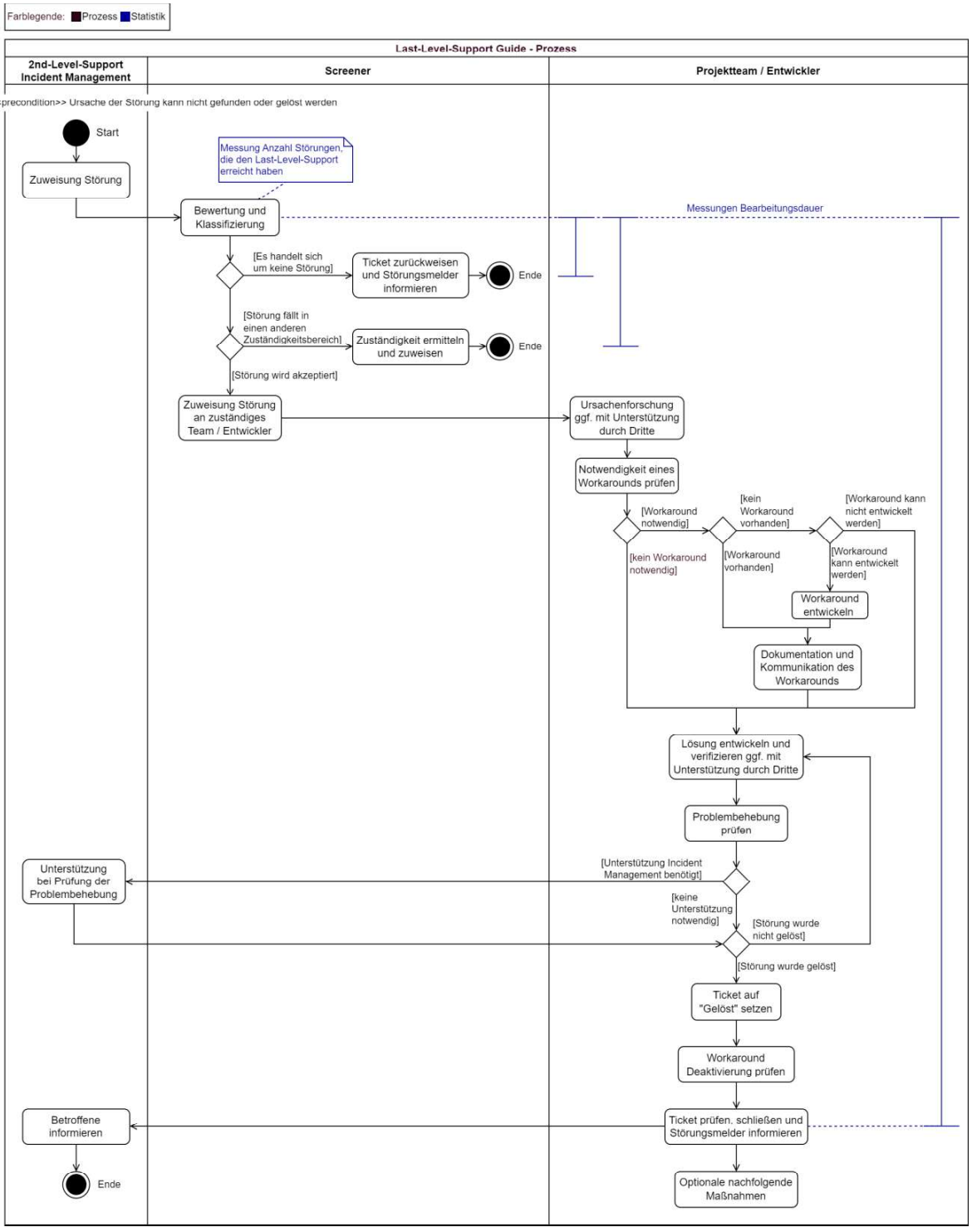
- [MUSS]: Eine Lösung muss entwickelt werden.
- [KANN]: Zur Entwicklung besteht wieder die Möglichkeit der Unterstützung durch Dritte (siehe entsprechenden Abschnitt im Kapitel Ursachenforschung).
- [MUSS]: Zuweisung der Störung an eine zuständige Person oder einen Personenkreis innerhalb der Software Engineering Abteilung.
- [KANN]: Für die Bearbeitung der Störung durch das entsprechende Entwicklungsteam kann ein Ticket im Aufgabenbacklog (z. B. Jira) des jeweiligen Projektes angelegt werden.
- [MUSS]: Implementierung der Lösung nach SWE-Framework (siehe Software Engineering Module).

4. Problembehebung prüfen

- [MUSS]: Es muss geprüft werden, ob die entwickelte Lösung die Störung behebt.
- [KANN]: Zur Überprüfung besteht wieder die Möglichkeit der Unterstützung durch Dritte (siehe entsprechenden Abschnitt im Kapitel Ursachenforschung). Ggf. ist die Unterstützung des Incident Managements notwendig. Entsprechend muss eine Abstimmung erfolgen.
- [MUSS]: Aktualisierung des Aufgabenbacklogs bzw. des Ticketsystems.
  - Workaround Deaktivierung prüfen: Falls zuvor zur Lösung ein Workaround angewendet wurde, muss geprüft werden, ob dieser in der Known Error Database deaktiviert werden muss. Weitere Informtionen stehen in der zur Arbeitsanweisung Known Error Datenbank verwalten.

5. Nachfolgende Maßnahmen

- [KANN]: Die Anfertigung eines separaten Berichts ist nicht zwingend erforderlich, da alle relevanten Informationen im Ticket dokumentiert sind. Daraus ergibt sich, dass Reports über relevante Kennzahlen, wie die Durchlaufzeiten (Mean Time to Repair / Recover), erstellt werden können
- [KANN]: Nach Bedarf Durchführung eines Lessons Learned Workshops:
  - Können Maßnahmen getroffen werden, damit Störungen dieser Art in Zukunft weniger bis gar nicht mehr auftreten?
  - Stichwort kontinuierlicher Verbesserungsprozess (siehe Kapitel Proaktiver Last-Level-Support).
- [EMPFOHLEN]: Wenn bestimmte Fehlerbilder häufig auftreten, sollten möglichst Automatismen implementiert werden, sogenannte Watch Dogs, die mögliche Fehlfunktionen der Software frühzeitig erkennen und melden.



4.7.4 Schulungen

Für Software Support ist zusätzlich notwendig, die Bedarfe hinsichtlich Schulungen frühzeitig zu identifizieren, um ein geeignetes Schulungskonzept zu entwickeln. Dabei gilt:

- [MUSS]: Zunächst muss der Schulungsbedarf identifiziert werden. Sollte eine Schulung benötigt werden, muss ein geeignetes Schulungskonzept erarbeitet werden unter Berücksichtigung der folgenden Punkte:
  - Komplexität des Produkts: Von Demonstrationen von einfachen Apps bis hin zu mehrtägigen Schulungen bei komplexeren militärischen Systemen.
  - Schulungen für die unterschiedlichen Nutzerkreise: Verschiedene Rollen wie Basic User, Power User, Administratoren usw. benötigen unterschiedliche Schulungsinhalte.
  - Anforderungen an das Schulungspersonal: Der Coach muss sowohl das Produkt als auch den Nutzerkreis und die relevanten Use Cases kennen.
  - Notwendigkeit einer Schulungsumgebung: Bei Bedarf Einrichtung einer entsprechenden Schulungsumgebung (getrennt von der Produktivumgebung) für das Produkt sowie Identifikation aller Anforderungen an eine Schulungsumgebung; Definieren und Einspielen von Schulungsdaten.
  - Schulungsmaterial: Je nach Komplexität des Softwareprodukts und Teilnehmerkreises Vorbereitung von Schulungsszenarien sowie Bereitstellung des Schulungsmaterial in digitaler Form oder Papierform.
  - Abstimmung mit Stakeholdern: Wenn die Software bei der Ausbildung von Soldaten eine Rolle spielt sind ggf. Stakeholder von Ausbildungsschulen oder UniBw einzubinden.
  - Schulungsnachweise/Teilnahmebescheinigungen: Spielt die Software z. B. für die Ausbildung von Soldaten eine Rolle, kann ein entsprechender Nachweis über die Kenntnisse der Software notwendig sein.
  - Berücksichtigung von ggf. existierenden Altsystemen: Vor allem bei der Entwicklung von Software, die bestehende Altsysteme ablöst, muss auch die abzulösende Software beachtet werden; Coach sollte Altsystem kennen, entsprechend in der Schulung darauf eingehen und mit Vorbehalten umgehen können.
  - Aktualisierung für neue Releases: Ggf. notwendige Schulungen zum "Auffrischen" oder Fortgeschrittenenkurse.

5 Glossar

5.1 Allgemeine Definitionen

Begriff	Erklärung
API - Application Programming Interface	Eine Schnittstellen-Spezifikation einer Software für die Interaktion mit anderen Komponenten bzw. Programm- oder Anwendungselementen. Weitere Informationen: Programmierschnittstelle – Wikipedia
Blue-Green Deployment	Eine Methode, um Änderungen an einem Server vorzunehmen, indem abwechselnd Produktions- und Staging-Server ausgetauscht werden. Weitere Informationen: Blue-green deployment - Wikipedia
CD - Continuous Delivery	Eine tool-gestützte Vorgehensweise, um neuen Code automatisiert und schneller zu veröffentlichen. Weitere Informationen: Continuous Lifecycle (bwi-intranet.de)
CD - Continuous Deployment	Eine Form der automatisierten Ausbringung in den Betrieb (Verteilung, Initialisierung, Erstbefüllung etc.) zum Nutzungsstart für den Kunden. Weitere Informationen: Continuous Lifecycle (bwi-intranet.de)
CI - Continuous Integration	Ein Verfahren, um fortlaufend Codeänderungen einzubringen, zu testen und zusammenzufügen. Weitere Informationen: Continuous Lifecycle (bwi-intranet.de)
Coding Guideline	Eine Coding Guideline umfasst die Konventionen zur Erstellung von Quellcode für eine spezifische Programmiersprache. Hierzu gehören u.a. Formatierung des Quellcodes, Benennung von Variablen und die Nutzung von Kommentaren. Die Nutzung einer Coding Guideline unterstützt die Einhaltung der sprachübergreifenden Clean-Code-Prinzipien. Begriffe wie Style Guide oder Coding Conventions werden häufig synonym zum Begriff Coding Guideline verwendet.
COTS	"Commercial off-the-shelf" sind seriengefertigte Softwareprodukte (Standardsoftware), die in großer Stückzahl völlig gleichartig aufgebaut und verkauft werden. Weitere Informationen: Commercial off-the-shelf – Wikipedia

Begriff	Erklärung
DevOps	DevOps beschreibt die crossfunktionale Bündelung von Entwicklungs-, Betriebs- und weiteren Leistungen, die durch technische und nicht-technische Merkmale geprägt ist. Das gemeinsame Ziel hierbei ist es, sichere Software in kurzen Release-Zyklen bereitzustellen. Die Begriffe DevOps und DevSecOps werden im Kontext des SWE Frameworks als Synonyme gesehen, da die Berücksichtigung der Security-Aspekte im professionellen Software Engineering als obligatorisch verstanden wird ("Security by Default", siehe: Architecture & Design). Weitere Informationen: DevOps (bwi-intranet.de)
Domain Driven Design	Vorgehensweise für den Entwurf eines Systems, das auf einen Wirkungsbereich (Domäne) spezialisiert ist. Die Fachlichkeit der Domäne wird in den Vordergrund gestellt, so dass alle beteiligten Personen ein gemeinsames Verständnis und eine gemeinsame Sprache ("Ubiquitous Language") bekommen. Weitere Informationen: Was ist Domain-Driven Design (DDD)? | heise Developer Domain-driven Design – Wikipedia
Epic	Eine große, umfangreiche User Story, die zu groß für die Umsetzung innerhalb eines Sprints ist und somit in kleinere User Storys aufgeteilt werden muss Weitere Informationen: Epic (Anforderungsmanagement) – Wikipedia
Git	Git ist eine freie Software zur verteilten Versionsverwaltung von Softwareartefakten bzw. Dateien. Weitere Informationen: Git (git-scm.com)
GitFlow	Gitflow ist ein Branching-Modell, dass sich zur Verwaltung größerer Projekte eignet. Weitere Informationen: A successful Git branching model » nvie.com
IDE - Integrierte Entwicklungsumgebung	Software für die Entwicklung von Anwendungen in einer (grafischen) Benutzeroberfläche. Weitere Informationen: Integrierte Entwicklungsumgebung – Wikipedia
KEDB - Known Error Database	Eine KEDB ist die Datenbank in der ITSM Suite, die sämtliche Dokumentationen bekannter Fehler enthält. Diese Datenbank wird vom Problem Management gemanagt und vom Incident Management sowie Problem Management eingesetzt. Die Known Error Database ist Teil des Service Knowledge Management Systems.

Begriff	Erklärung
	Übernommen aus dem BWI Glossar: https://www.sp.bwi-intranet.de/app/00005/glossar/Seiten/Glossar.aspx?title=Known%20Error%20Database%20(Wissensdatenbank) Die ITSM Suite der BWI besteht aus Maximo in Kombination mit IT-SPS.
KISS	Abkürzung für das englische "Keep it simple and stupid": Prinzip, zu einem Problem eine möglichst einfache Lösung anzustreben. Weitere Informationen: KISS-Prinzip – Wikipedia
MOTS	"Modifiable off-the-shelf" beschreibt ein Standardsoftwareprodukt, das auf individuelle Bedürfnisse angepasst werden kann, z. B. durch Offenheit des Quelltextes. Weitere Informationen: Modifiable off-the-shelf – Wikipedia
MLOps - Machine Learning Operations	MLOps beschreibt in Anlehnung an DevOps ein Konzept zum Lifecycle-Management einer Software-Applikation, die im Kern Machine Learning Modelle benutzt.
MVP - Minimum Viable Product	Eine erste, benutzbare, frühzeitig bereitgestellte Version eines neuen Produkts nur mit den nötigsten Kernfunktionen, die mit geringem Aufwand erstellt wurde mit dem Ziel, Kundenfeedback zu sammeln. Weitere Informationen: Minimum Viable Product – Wikipedia Was ein gutes MVP ausmacht - Andreas Diehl (#DNO) (digitaleneuordnung.de)
Open Source	Open Source Software ist öffentlicher Quellcode, so dass er von Außenstehenden eingesehen, geändert und genutzt werden kann. Meistens kann die Software kostenlos genutzt werden. Weitere Informationen: Open Source – Wikipedia
Prototyp bzw. Prototypische Anwendung	Ein Prototyp ist ein lauffähiges Software-Artefakt oder eine anderweitige konkrete Modellierung (z. B. Mock-up) einer Teilkomponente des Softwareproduktes und dient als Basis für die folgende Entwicklung des Softwareproduktes. Der Prototyp kann auch als Basis für eine bessere Kommunikation mit den Kunden oder auch innerhalb des Entwicklungsteams über konkrete Dinge (statt abstrakte Modelle) dienen. Weitere Informationen: Prototyping (Softwareentwicklung) – Wikipedia
Release	Die fertige und veröffentlichte Version bzw. Kundenversion einer Software, manchmal auch als Hauptversion bezeichnet. Weitere Informationen: Entwicklungsstadium (Software) – Wikipedia

Begriff	Erklärung
Releaseprozess	Vorgang, der zu einem Softwarepaket bzw. mehreren Softwareartefakten (Release, Release Candidate) mit spezieller Versionsnummer führt. Weitere Informationen: Releasemanagement – Wikipedia
SCCM - System Center Configuration Manager	Ein Softwareprodukt von Microsoft um die Verwaltung von Hard- und Software innerhalb eines Unternehmens zu zentralisieren. Es wird insbesondere zur Softwareverteilung benutzt. Weitere Informationen: System Center Configuration Manager – Wikipedia
SoC - Separation of concerns	Ein Softwarearchitektur-Design-Pattern, bei dem die verschiedenen Zuständigkeiten einer Anwendung auf einzelne Bestandteile aufgeteilt und umgesetzt werden. Weitere Informationen: Separation of concerns - Wikipedia
SOLID	Akronym für fünf Designprinzipien in der objektorientierten Softwareentwicklung: ▪ Single-responsibility principle ▪ Open-closed principle ▪ Liskov substitution principle ▪ Interface segregation principle ▪ Dependency inversion principle Weitere Informationen: Principles of Ood (butunclebob.com)
SonarQube	Eine Open-Source-Plattform für statistische Analysen zur Prüfung und Bewertung der technischen Qualität von Quellcode. Weitere Informationen: Code Quality and Code Security | SonarQube
SWAG	"Scientific Wildly Aimed Guess" steht für eine grobe Schätzung basierend auf der Erfahrung der Software Engineering Expert*innen.
SWE	Die BWI-Einheit "CoE Software Engineering".
Test Driven Development	Ein Softwareentwicklungsverfahren, bei dem zuerst die Testfälle entwickelt und ggf. automatisiert werden. Anschließend wird der funktionale Source Code zu den Testfällen entwickelt, um diese Testfälle zu bestehen. Weitere Informationen: ISTQB - Testgetriebene Entwicklung Testgetriebene Entwicklung – Wikipedia
UML - Unified Modeling Language	Grafische Modellierungssprache zur Spezifikation, Dokumentation und Visualisierung von Softwaresystemen. Weitere Informationen: Was ist die UML? - Wissen kompakt - t2informatik

Begriff	Erklärung
User Story	Eine kurze, in Alltagssprache formulierte Softwareanforderung aus Sicht eines Benutzers oder einer Benutzerin, meist unter Verwendung der Vorlage: "Als <Rolle/Kundentyp> möchte ich <Ziel/Wunsch>, um/damit <Nutzen>". Weitere Informationen: User Story – Wikipedia
Validation	Validierung überprüft, ob das Softwareprodukt den beabsichtigten Verwendungszweck erfüllt: Wird das richtige Softwareprodukt erstellt? Weitere Informationen: Software verification and validation - Wikipedia
Version	Ein hinsichtlich Softwareeigenschaften definiertes Entwicklungsstadium einer Software und aller dazugehörigen Komponenten. Weitere Informationen: Version (Software) – Wikipedia
WIR - Wissensrecord	Wissensrecords sind Einträge in der Wissensdatenbank. Wissensrecords werden erstellt, um Informationen zu verschiedenen fachlichen Themen zur Verfügung zu stellen. Das Ziel dieser Wissensrecords ist, Serviceanfragen, Vorfälle oder Probleme möglichst schnell und in gleichbleibender Qualität zu bearbeiten. Diese Informationen können sein: ▪ Lösung zu einer Störung/Problem (WIR vom Typ „Lösung“). ▪ Provisorische Lösung zu einer Störung/Problem (WIR vom Typ „Workaround“). ▪ Auslösung eines Standardchanges z. B. bei Bestellungen (WIR vom Typ „RfC“). ▪ Allgemeine Informationen für die weitere Bearbeitung eines Tickets oder Anleitungen (How To, WIR vom Typ „Information“). Übernommen aus dem BWI Glossar: https://www.sp.bwi-intranet.de/app/00005/glossar/Seiten/Glossar.aspx?title=Wissensrecord

5.2 Definitionen und Hintergrundwissen zu Software Quality & Assurance

Agiles Testen

Definition: ISTQB

Als integraler Bestandteil des Softwareentwicklungsprozesses unterteilt Agiles Vorgehen den Entwicklungsprozess in kleinere Teile, Iterationen und Sprints. Dadurch können die Tester*innen während des gesamten Prozesses parallel mit dem Rest des Teams arbeiten und die Mängel und Fehler sofort nach ihrem Auftreten beheben.

Der Hauptzweck eines solchen Prozesses besteht darin, neue Softwarefunktionen schnell und mit der besten Qualität zu liefern. Daher ist dieser Ansatz auch weniger kostenintensiv: Die Behebung von Fehlern in einem frühen Stadium des Entwicklungsprozesses, bevor weitere Probleme auftreten, ist wesentlich kostengünstiger und erfordert weniger Aufwand.

Beim agilen Testansatz geht es eher um den Aufbau einer QA-Praxis als um ein QA-Team. Die Qualitätssicherung sollte in agilen Projekten z. B. in Scrum-Teams eingebettet sein, anstatt in separaten Teams durchgeführt zu werden. Dadurch entsteht eine effiziente Kommunikation innerhalb des Teams und durch die aktive Einbeziehung der Beteiligten wird der Prozess beschleunigt und besser informierte Entscheidungen werden getroffen.

Teststrategie

Definition: ISTQB

Eine Teststrategie liefert eine verallgemeinernde Beschreibung des Testprozesses, üblicherweise auf Produkt- oder Organisationsebene. Gängige Arten von Teststrategien sind u.a.: Analytisch, Modellbasiert, Methodisch, Prozesskonforme (oder Standardkonforme), Angeleitete (oder beratende), Regressionsvermeidend (Regression-avers) und Reaktiv. Eine angemessene Teststrategie wird häufig durch die Kombination dieser verschiedenen Arten von Teststrategien erstellt.

"Eine Teststrategie definiert die Testziele und die Maßnahmen, die geeignet erscheinen, diese zu erreichen. Sie bestimmt damit den Testaufwand und die Testkosten. Ziel dabei ist es, einen Maßnahmenmix zu finden, der die Relation zwischen Testkosten und drohenden Fehlerkosten optimiert und das Risiko minimiert." (Quelle: Andreas Spillner und Tilo Linz, Basiswissen Softwaretest, dpunkt.verlag). Präventive Methoden sind bei neuen Produkten zu bevorzugen.

Testplan

Definition: ISTQB

Während es sich bei einem Testkonzept um ein übergeordnetes Dokument handelt, hat der Testplan einen eher praktischen Ansatz, der detailliert beschreibt, was getestet werden soll, wie getestet werden soll, wann getestet werden soll und wer den Test durchführen wird. Im Gegensatz zum statischen Testkonzept, das sich auf ein Projekt als Ganzes bezieht, deckt der Testplan jede Testphase einzeln ab und wird vom Projektleiter während des gesamten Prozesses häufig aktualisiert.

Die ISTQB-Definition für den Testplan lautet: "Eine Liste von Aktivitäten, Aufgaben oder Ereignissen des Testprozesses, mit Angabe ihrer geplanten Anfangs- und Endtermine sowie ihrer gegenseitigen Abhängigkeiten."

Testentwurf

Definition: ISTQB

Während des Testentwurfs werden die Testbedingungen in abstrakte Testfälle, Sets aus abstrakten Testfällen und andere Testmittel überführt. Der Testentwurf beantwortet die Frage: „Wie wird getestet?“.
Der Testentwurf beinhaltet die folgenden Hauptaktivitäten:

- Entwurf und Priorisierung von Testfällen und Sets an Testfällen.
- Identifizierung von notwendigen Testdaten zur Unterstützung der Testbedingungen und Testfälle.
- Entwurf der Testumgebung und Identifizierung benötigter Infrastruktur und Werkzeuge.
- Erfassung der bidirektionalen Verfolgbarkeit zwischen der Testbasis, den Testbedingungen und den Testfällen.

Testdurchführung

Definition: ISTQB

Die Aktivität der Ausführung eines Tests für eine Komponente oder ein System, die Ist-Ergebnisse erzeugt. Während der Testdurchführung laufen Testsuiten in Übereinstimmung mit dem Testausführungsplan ab.

Einige Hauptaktivitäten der Testdurchführung sind:

- Durchführung der Tests entweder manuell oder durch Nutzung von Testausführungswerkzeugen.
- Vergleich der Ist-Ergebnisse mit den erwarteten Ergebnissen.
- Bericht über Fehlerzustände auf Grundlage der beobachteten Fehlerwirkungen.
- Aufzeichnung der Ergebnisse der Testdurchführung (z. B. bestanden, fehlgeschlagen, blockiert).

Das Statische Testen ist das Testen von Software-Entwicklungsartefakten, z. B. Anforderungen oder Quelltext, ohne diese auszuführen, z. B. durch Reviews oder statische Analyse. Reviews können auf jedes Arbeitsergebnis angewendet werden, von dem die Teilnehmer*innen wissen, wie es zu lesen und zu verstehen ist. Statische Analysen können effizient auf jedes Arbeitsergebnis mit einer formalen Struktur angewendet werden (üblicherweise Code oder Modelle), für die es ein geeignetes statisches Analysewerkzeug gibt. Einige Statische Tests sind: Überprüfung von Condinf Guidelines, Überprüfung von Source-Code-Metriken und Analyse zur Erkennung von Laufzeitfehlern.

Das Dynamische Testen ist die Prüfung des Testobjekts durch Ausführung auf einem Rechner. Die größte Stärke des dynamischen Tests liegt im systematischen Nachweis der Funktionalität des entwickelten Systems bzw. der Software. Es gibt, im Vergleich zum dynamischen Test, bis heute keine auch nur annähernd so effektive statische Methode, um die Korrektheit der implementierten Funktionalität nachzuweisen. Hier werden dann Komponententests, Integrationstests, Systemtests und Abnahmetests ausgeführt.

Testprozess

Definition: ISTQB

Es gibt nicht den einen universellen Softwaretestprozess, aber es gibt eine Reihe von gebräuchlichen Testaktivitäten. Ohne diese Aktivitäten erreicht das Testen die festgelegten Ziele mit einer weit geringeren Wahrscheinlichkeit. Die Menge von Testaktivitäten bildet den Testprozess. Der geeignete, spezifische Softwaretestprozess in einer vorgegebenen Situation hängt von vielen Faktoren ab. Welche Testaktivitäten in diesem Testprozess beinhaltet sind, wie diese Aktivitäten eingesetzt werden und wann diese Aktivitäten stattfinden, kann in der Teststrategie eines Unternehmens behandelt werden.

Ein Testprozess besteht aus den folgenden Hauptgruppen von Aktivitäten:

- Testplanung
- Testüberwachung und -steuerung
- Testanalyse
- Testentwurf
- Testrealisierung
- Testdurchführung
- Testabschluss

Teststufen

Definition: ISTQB

Laut ISTQB sind Teststufen spezifische Instanziierungen eines Testprozesses. Jede Teststufe betrachtet unterschiedliche Teile einer Software. Jede Teststufe ist ein wichtiges Puzzleteil für den Qualitätserfolg und sollte nicht vernachlässigt werden.

Die gängigsten Teststufen sind Komponententest, Integrationstest, Systemtest und Abnahmetest.

	Komponententest	Integrationstest	Systemtest	Abnahmetest
Was	Konzentriert sich auf Komponenten, die einzeln testbar sind.	Konzentriert sich auf die Interaktion zwischen den Komponenten oder Systemen.	Konzentriert sich auf das Verhalten und die Fähigkeiten des Systems oder Produkts unter Berücksichtigung der E2E Aufgaben und der nicht funktionalen Verhaltensweisen.	Konzentriert sich darauf, wie der Systemtest typischerweise auf das Verhalten und die Fähigkeiten eines gesamten Systems oder Produkts reagiert.

	Komponententest	Integrationstest	Systemtest	Abnahmetest
Warum/Fokus	Stellt sicher, dass der Code korrekt entwickelt wurde.	Stellt sicher, dass die Interaktion zwischen den Komponenten wie gewünscht funktioniert.	Stellt sicher, dass das gesamte System gut funktioniert, nachdem es integriert ist. In Bezug auf die Anforderungen.	Stellt sicher, dass das System die Anforderungen der Benutzer*innen erfüllt oder nicht, in Bezug auf Stories und Features.
Tools (Beispiele)	JUnit, TestNG, NUnit, Mockito, PHPUnit, XCTest	SoapUI, Parasoft SOATest, Katalon Studio	Appium, Selenium, XCUITest, Kaspresso, Katalon Studio	Appium, Selenium, XCUITest, Kaspresso, Katalon Studio

Testarten

Definition: ISTQB

Eine Testart ist eine Gruppe von Testaktivitäten, die darauf abzielt, spezifische Merkmale eines Softwaresystems oder eines Teils eines Systems auf der Grundlage spezifischer Testziele zu testen. Es gibt folgende Testarten: Funktionale Tests, Nicht-funktionale Tests, White-Box-Tests, Änderungsbezogene Tests. Einige Ziele könnten folgende sein: Bewertung funktionaler Qualitätsmerkmale wie Vollständigkeit, Korrektheit und Angemessenheit, Bewertung nicht-funktionaler Qualitätsmerkmale wie Zuverlässigkeit, Performanz, IT-Sicherheit, Kompatibilität und Gebrauchstauglichkeit (Usability).

Funktionale Tests: Bei funktionalen Tests wird das System anhand der funktionalen Anforderungen getestet, indem Eingaben gemacht und die Ausgaben untersucht werden. Dieser Aspekt konzentriert sich auf die praktische Nutzung der Software aus der Sicht der Benutzer*innen: Funktionen, Leistung, Benutzerfreundlichkeit, Fehlerfreiheit. Bei dieser Art der Prüfung wird die Black-Box-Methode angewandt. Das bedeutet, dass nicht die Verarbeitung selbst, sondern deren Ergebnisse im Vordergrund stehen.

Nicht-funktionale-Tests: Bei Nicht-funktionalen Tests werden die inneren Merkmale und die Architektur des Systems, d. h. die strukturellen (impliziten) Anforderungen getestet. Dazu gehört die Wartbarkeit, Verständlichkeit, Effizienz und Sicherheit des Codes.

White-Box-Tests: White-Box-Tests sind die detaillierte Untersuchung der internen Logik und Struktur des Codes. Um White-Box-Tests an einer Anwendung durchführen zu können, müssen Tester*innen die interne Funktionsweise des Codes kennen.

Black-Box-Tests: Die Technik des Testens ohne Kenntnis der inneren Funktionsweise der Anwendung. Tester*innen kennen die Systemarchitektur nicht und haben keinen Zugriff auf den Quellcode. In der Regel interagieren Tester*innen bei der Durchführung eines Black-Box-Tests mit der Benutzeroberfläche des Systems, indem sie Eingaben machen und die Ausgaben untersuchen, ohne zu wissen, wie und wo die Eingaben verarbeitet werden.

Grey-Box-Tests: Ist eine Technik zum Testen der Anwendung mit einem begrenzten Wissen über die interne Funktionsweise einer Anwendung. Im Gegensatz zu Black-Box-Tests hat man zusätzlich bei Grey-Box-Tests Zugang zu den Designdokumenten und der Datenbank. Mit diesem Wissen können Tester*innen bei der Erstellung eines Testplans bessere Testdaten und Testszenarien vorbereiten.

Änderungsbezogene Tests: Es soll bei änderungsbezogenen Tests überprüft werden, ob Änderungen am System korrekt durchgeführt wurden und keine negativen Auswirkungen auf das System haben.

5.3 Definitionen zu UX/UI Design

User Experience

Die User Experience (UX) ist die Gesamtheit der Erfahrungen, die ein*e Anwender*in durch eine Interaktion mit einer Anwendung macht. Sie umfasst alle Wahrnehmungen und Reaktionen einer Benutzerin oder eines Benutzers, die sich aus der Benutzung und/oder der erwarteten Benutzung eines interaktiven Systems ergeben (z. B. Emotionen, Überzeugungen, Vorlieben und Verhaltensweisen der Benutzerin oder des Benutzers die *vor, während und nach der Benutzung* auftreten).

UX wird beeinflusst von:

- Markenimage, Präsentation, Funktionalität, Systemleistung.
- Interaktivem Verhalten und unterstützenden Fähigkeiten des interaktiven Systems.
- Erfahrungen, Einstellungen, Fähigkeiten und Persönlichkeit der Benutzerin oder des Benutzers (psychischer und physischer Zustand).
- Nutzungskontext.

UX **= Zufriedenstellung + Erfüllung von Erwartungen der Nutzerin oder des Nutzers** *(vor, während und nach der Benutzung).*

User Interface

Das User Interface (UI) beinhaltet die Elemente einer Benutzerschnittstelle, die der Benutzerin oder dem Benutzer vom interaktiven System präsentiert werden. UI-Elemente sind die Grundlage für die Erstellung der Funktionen, die Benutzer*innen benötigen, um Aufgaben zu erledigen. „Form follows function” als Design-Prinzip und damit gute Benutzbarkeit und Software-Ergonomie stehen dabei im Fokus.

UI wird beeinflusst von:

- Nutzungsanforderungen
- Informationsarchitektur
- Dialogprinzipien
- Gestaltungsregeln
- Heuristiken

UI = Benutzerschnittstelle zwischen Mensch und interaktivem System.

Usability

Usability bezeichnet das Ausmaß, in dem ein interaktives System durch bestimmte Benutzer*innen in einem bestimmten Nutzungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen (während der tatsächlichen Benutzung).

Usability wird beeinflusst von:

- Erfahrungen, Einstellungen, Fähigkeiten und Persönlichkeit der Benutzerin oder des Benutzers (psychischer und physischer Zustand).
- Ziele und Aufgaben.
- Nutzungskontext.
- Technische Gegebenheiten (z. B. technische Mängel können zu Usability-Problemen führen, wenn sie verhindern, dass Benutzer*innen ihre Aufgaben effektiv oder effizient lösen können).

Usability = Effektivität + Effizienz + Zufriedenstellung *(während der tatsächlichen Benutzung).*

Design System

Ein Design System ist eine Sammlung von User-Interface-Elementen. Es wird verwendet, um Konsistenz in der Darstellung und im Verhalten von Benutzungsschnittstellen in allen interaktiven Systemen zu gewährleisten, die von derselben Organisation erstellt werden. Ein darin enthaltenes Design Pattern ist eine allgemeine Lösung für ein häufig auftretendes Problem innerhalb eines gegebenen Kontextes. Ein Styleguide hingegen ist eine Sammlung von Gestaltungsregeln.

Design System = Sammlung + Anwendungsvorgaben von UI Elementen.

5.4 Definitionen zu AI Applications

Experimentation / Experiment Tracking

Mit der Fähigkeit zum "Experiment Tracking" können Data Scientists und ML-Forscher*innen gemeinsam explorative Datenanalysen durchführen, prototypische ML/KI-Modellarchitekturen erstellen und Trainingsroutinen implementieren. Eine ML-Umgebung sollte auch ermöglichen, modularen, wiederverwendbaren und testbaren Quellcode zu schreiben, der versionskontrolliert ist. Zu den wichtigsten Funktionen beim Experimentieren gehören die folgenden:

- Bereitstellung von Notebook-Umgebungen, die mit Versionskontrollwerkzeugen wie Git integriert sind.
- Nachverfolgung von Experimenten, einschließlich Informationen zu den Daten, Hyperparametern und Auswertungsmetriken für Reproduzierbarkeit und Vergleichbarkeit.
- Analyse und Visualisierung von Daten und Modellen.
- Unterstützung bei der Erkundung von Datensätzen, der Suche nach Experimenten und der Überprüfung von Implementierungen. Integration mit anderen Datendiensten und ML-Diensten in einer Plattform.

Data Processing

Mit der Fähigkeit zum "Data Processing" bzw. der Datenverarbeitung können große Datenmengen für die ML-Entwicklung, für kontinuierliche Trainingspipelines und für die Vorhersage aufbereitet und transformiert werden. Zu den wichtigsten Funktionen der Datenverarbeitung gehören:

- Unterstützung der interaktiven Ausführung (z. B. von Notebooks) für schnelle Experimente und für lang laufende Jobs in der Produktion.
- Bereitstellung von Datenkonnektoren für ein breites Spektrum von Datenquellen und -diensten sowie von Datenkodierern und -dekodierern für verschiedene Datenstrukturen und
  Dekodierer für verschiedene Datenstrukturen und -formate.
- Bereitstellung von umfangreichen und effizienten Datentransformationen und ML-Feature-Engineering für strukturierte (tabellarische) und unstrukturierte Daten (Text, Bild usw.).
- Unterstützung skalierbarer Batch- und Stream-Datenverarbeitung für ML-Training und Serving-Workloads.

Model Training

Mit der Fähigkeit zum "Model Training" kann man effizient und kostengünstig leistungsstarke Algorithmen für das Training von ML-Modellen ausführen.
Das Model Training sollte sowohl mit der Modell- als auch mit der Trainingsdatensatzgröße skalieren können. Zu den wichtigsten Funktionen des Model Training gehören:

- Unterstützung gängiger ML-Frameworks und Unterstützung benutzerdefinierter Laufzeitumgebungen.
- Unterstützung eines groß angelegten verteilten Trainings mit verschiedenen Strategien für mehrere GPUs und mehrere Worker.

- Möglichkeit für bedarfsgerechte Nutzung von ML-Beschleunigern.
- Möglichkeit für effizientes Tuning von Hyperparametern und eine Zieloptimierung im großen Maßstab.
- Idealerweise Bereitstellung integrierter automatisierter ML-Funktionen (AutoML), einschließlich automatischer Auswahl und Entwicklung von Features sowie automatischer Suche und Auswahl der Modellarchitektur.

Model Testing / Model Evaluation

Mit der Fähigkeit "Model Testing / Model Evaluation" kann die Wirksamkeit eines Modells interaktiv während des Experimentierens und automatisch in der Produktion bewertet werden. Zu den wichtigsten Funktionen der Modellevaluation gehören:

- Durchführung von Batch-Scoring der Modelle auf Evaluationsdatensätzen in großem Umfang.
- Berechnung von vordefinierten oder benutzerdefinierten Bewertungsmetriken für das Modell auf verschiedenen Teilmengen des Datensatzes.
- Verfolgen der Vorhersageleistung des trainierten Modells über verschiedene kontinuierliche Trainingsausführungen hinweg.
- Visualisieren und Vergleichen der Leistung von verschiedenen Modellen.
- Bereitstellung von Werkzeugen für "Was-wäre-wenn"-Analysen und zur Ermittlung von Verzerrungen / Bias und Fairnessproblemen.
- Möglichkeit der Interpretation des Modellverhaltens durch verschiedene "Explainable-AI"-Techniken.

Model Serving

Mit der Fähigkeit zum "Model Serving" können trainierte ML-Modelle in Produktionsumgebungen eingesetzt und bereitgestellt werden. Zu den wichtigsten Funktionen des Model Serving gehören:

- Unterstützung für Vorhersagen mit niedriger Latenz und nahezu in Echtzeit (online) sowie für Batch-Vorhersagen mit hohem Durchsatz (offline).
- Integrierte Unterstützung für gängige ML-Serving-Frameworks (z. B. TensorFlow Serving, TorchServe, Nvidia Triton und andere für Scikit-learn- und XGBoost-Modelle) sowie für benutzerdefinierte Laufzeitumgebungen.
- Ermöglichung zusammengesetzter Vorhersageroutinen, bei denen mehrere Modelle hierarchisch oder gleichzeitig aufgerufen werden, bevor die Ergebnisse aggregiert werden, zusätzlich zu allen erforderlichen Vor- oder Nachverarbeitungsroutinen.
- Ermöglichung einer effizienten Nutzung von ML-Inferenzbeschleunigern mit automatischer Skalierung zur Anpassung an spiky Workloads und zum Ausgleich von Kosten und Latenzzeit.
- Unterstützung der Erklärbarkeit von Modellen durch Techniken wie Feature-Attributionen für eine bestimmte Modellvorhersage.
- Unterstützung der Protokollierung von Anfragen und Antworten auf Vorhersagen zu Analysezwecken.

Online Experimente

Mit der Fähigkeit für "Online-Experimente" kann man herausfinden, wie neu trainierte ML-Modelle im Vergleich zu den aktuellen Modellen (falls vorhanden) in der Produktion abschneiden, bevor das neue Modell für die Produktion freigegeben wird. Mit Hilfe einer kleinen Teilmenge der Nutzerpopulation können beispielsweise die Auswirkungen eines neuen Empfehlungssystems auf die Klickrate und die Konversationsrate untersucht werden. Die Ergebnisse der Online-Experimente sollten in die "Model Registry" integriert werden, um die Entscheidung über die Freigabe des Modells für die Produktion zu erleichtern. Online-Experimente erhöhen die Zuverlässigkeit der ML-Freigaben, indem sie dabei helfen, schlecht funktionierende Modelle zu verwerfen und gut funktionierende Modelle zu fördern. Zu den wichtigsten Funktionen der Online-Experimente gehören:

- Unterstützung von Canary- und Shadow-Deployments.
- Unterstützung von Traffic-Splitting und A/B-Tests.
- Unterstützung von mehrarmigen Bandit-Tests (multi-armed bandit, MAB).

Model Monitoring

Mit der Fähigkeit zum "Model Monitoring" können die Effizienz und Effektivität der in der Produktion eingesetzten Modelle verfolgt werden, um die Qualität der Vorhersagen sicherzustellen. Diese Funktion alarmiert, wenn Modelle veraltet sind und untersucht und aktualisiert werden müssen. Zu den wichtigsten Funktionen des Model Monitoring gehören:

- Messung von Modelleffizienzmetriken wie Latenz und Auslastung der Serving-Ressourcen.
- Erkennen von Data Skews, einschließlich Schemaanomalien sowie Daten- und Konzeptverschiebungen und -abweichungen.
- Kombination des Model Monitoring mit der Model Evaluation zur kontinuierlichen Bewertung der Effektivität und Performance des eingesetzten Modells, falls Ground-Truth-Labels verfügbar sind.

ML Pipelines

Mit ML-Pipelines können komplexe ML-Trainings- und Vorhersage-Pipelines in der Produktion instrumentieren, orchestrieren und automatisieren. ML-Workflows koordinieren verschiedene Komponenten, wobei jede Komponente eine bestimmte Aufgabe in der Pipeline ausführt. Zu den wichtigsten Funktionen von ML-Pipelines gehören:

- Auslösung von Pipelines nach Bedarf, nach einem Zeitplan oder als Reaktion auf bestimmte Ereignisse.
- Aktivierung der lokalen interaktiven Ausführung zum Debuggen während der ML-Entwicklung.
- Kombination mit der Fähigkeit zum "ML-Metadaten-Tracking" zur Erfassung von Pipeline-Ausführungsparametern und zur Erstellung von Artefakten.
- Bietet eine Reihe integrierter Komponenten für gängige ML-Aufgaben und erlaubt auch benutzerdefinierte Komponenten.
- Ausführung in verschiedenen Umgebungen, einschließlich lokaler Rechner und skalierbarer Cloud-Plattformen.
- Optional können GUI-basierte Tools für den Entwurf und die Erstellung von Pipelines bereitgestellt werden.

Model Registry / Versionierung von Modellen

Mit einer Model Registry kann der Lebenszyklus der ML-Modelle in einem zentralen Repository verwaltet werden. Dies sichert die Qualität der Produktionsmodelle und ermöglicht es eine Übersicht über alle vorhandenen Modelle zu erhalten. Zu den wichtigsten Funktionen der Model Registry gehören:

- Registrieren, organisieren, verfolgen und versionieren Sie Ihre trainierten und eingesetzten ML-Modelle.
- Speichern von Modell-Metadaten und Laufzeit-Abhängigkeiten für die Einsatzfähigkeit.
- Pflege der Modelldokumentation und -berichterstattung, z. B. mithilfe von Modellkarten.
- Integration in die Modellevaluierungs- und Bereitstellungsfunktion und Verfolgung von Online- und Offline-Evaluierungsmetriken für die Modelle.
- Steuerung des Prozesses zur Einführung von Modellen: Überprüfung, Genehmigung, Freigabe und Rücknahme. Diese Entscheidungen basieren auf einer Reihe von Offline-Leistungs- und Fairness-Metriken sowie auf Online-Experimentierergebnissen.

Dataset and Feature Repository / Feature Engineering

Mit einem Datensatz- und Feature-Repository können die Definition und Speicherung von ML-Datenbeständen vereinheitlicht werden. Ein zentrales Repository mit frischen, hochwertigen Datenbeständen ermöglicht die gemeinsame Nutzung, Auffindbarkeit und Wiederverwendbarkeit. Das Repository bietet außerdem Datenkonsistenz für Training und Inferenz. Dies hilft Data Scientists und ML-Forscher*innen, Zeit bei der Datenvorbereitung und dem Feature-Engineering zu sparen, die in der Regel einen erheblichen Teil ihrer Arbeitszeit in Anspruch nehmen. Zu den wichtigsten Funktionen eines Datensatz- und Feature-Repositorys gehören:

- Ermöglichung der gemeinsamen Nutzung, Auffindbarkeit, Wiederverwendbarkeit und Versionierung von Datenbeständen.
- Ermöglichung von Echtzeit-Ingestion und Serving mit niedriger Latenz für Event-Streaming und Online-Vorhersage-Workloads.
- Batch-Ingest und -Serving mit hohem Durchsatz für ETL-Prozesse (Extrahieren, Transformieren, Laden) und Modelltraining sowie für Scoring-Workloads.
- Ermöglichung der Funktionsversionierung für Point-in-Time-Abfragen.
- Unterstützung verschiedener Datenmodalitäten, einschließlich Tabellendaten, Bilder und Text.

ML-Datenbestände können auf der Ebene ihrer Features oder auf der Ebene des gesamten Datensatzes verwaltet werden. Ein Feature-Repository könnte beispielsweise eine Entität namens "Kunde" enthalten, die Merkmale wie "Altersgruppe", "Postleitzahl" und "Geschlecht" umfasst. Andererseits könnte ein Datensatz-Repository einen Datensatz zur Kundenabwanderung enthalten, der Merkmale aus den Entitäten "Kunde" und "Produkt" sowie Ereignisprotokolle zu Käufen und Web-Aktivitäten umfasst.

ML Metadata & Artefakt Tracking

In den verschiedenen Stufen des MLOps-Lifecycles werden verschiedene Arten von ML-Artefakten erstellt, darunter beschreibende Statistiken und Datenschemata, trainierte Modelle und Bewertungsergebnisse. ML-Metadaten sind die Informationen über all diese Artefakte, einschließlich ihres Speicherorts, ihrer Typen, Eigenschaften und Zuordnungen zu Experimenten und Läufen. Die Fähigkeit zur Verfolgung / Tracking von ML-Metadaten und -Artefakten ist die Grundlage für alle anderen MLOps-Funktionen. Eine solche Fähigkeit ermöglicht die Reproduzierbarkeit und Fehlersuche bei komplexen ML-Aufgaben und Pipelines. Zu den wichtigsten Funktionen der ML-Metadaten- und Artefaktverfolgung gehören:

- Rückverfolgbarkeit und Nachverfolgung der Herkunft von ML-Artefakten.
- Gemeinsame Nutzung und Tracking von Experimenten und Pipeline-Parameter-Konfigurationen.
- Speichern, Zugreifen, Untersuchen, Visualisieren, Herunterladen und Archivieren von ML-Artefakten.
- Integration mit allen anderen MLOps-Funktionen.

6 Verweise auf andere Dokumente

6.1 Anlagen

[1] Orientierungshilfe Informationssicherheit

[2] Checkliste Software Engineering Framework

[3] Template Aufwandsschätzung

[4] Template README

[5] Java EditorConfig

[6] JavaScript EditorConfig

[7] Python EditorConfig

Sämtliche Anlagen sind unter folgender Adressen abrufbar:

- aus dem BWI-Netz:
  https://social.sp.bwi-intranet.de/groups/471/Pages/Wiki/Software%20Engineering%20Framework.aspx

- aus dem Bw- und dem BWI-Netz:
  https://nextcloud4bwi.de/index.php/f/2918073

6.2 Mitgeltende Dokumente

CON.8 Software-Entwicklung (bund.de)

6.3 Quellen

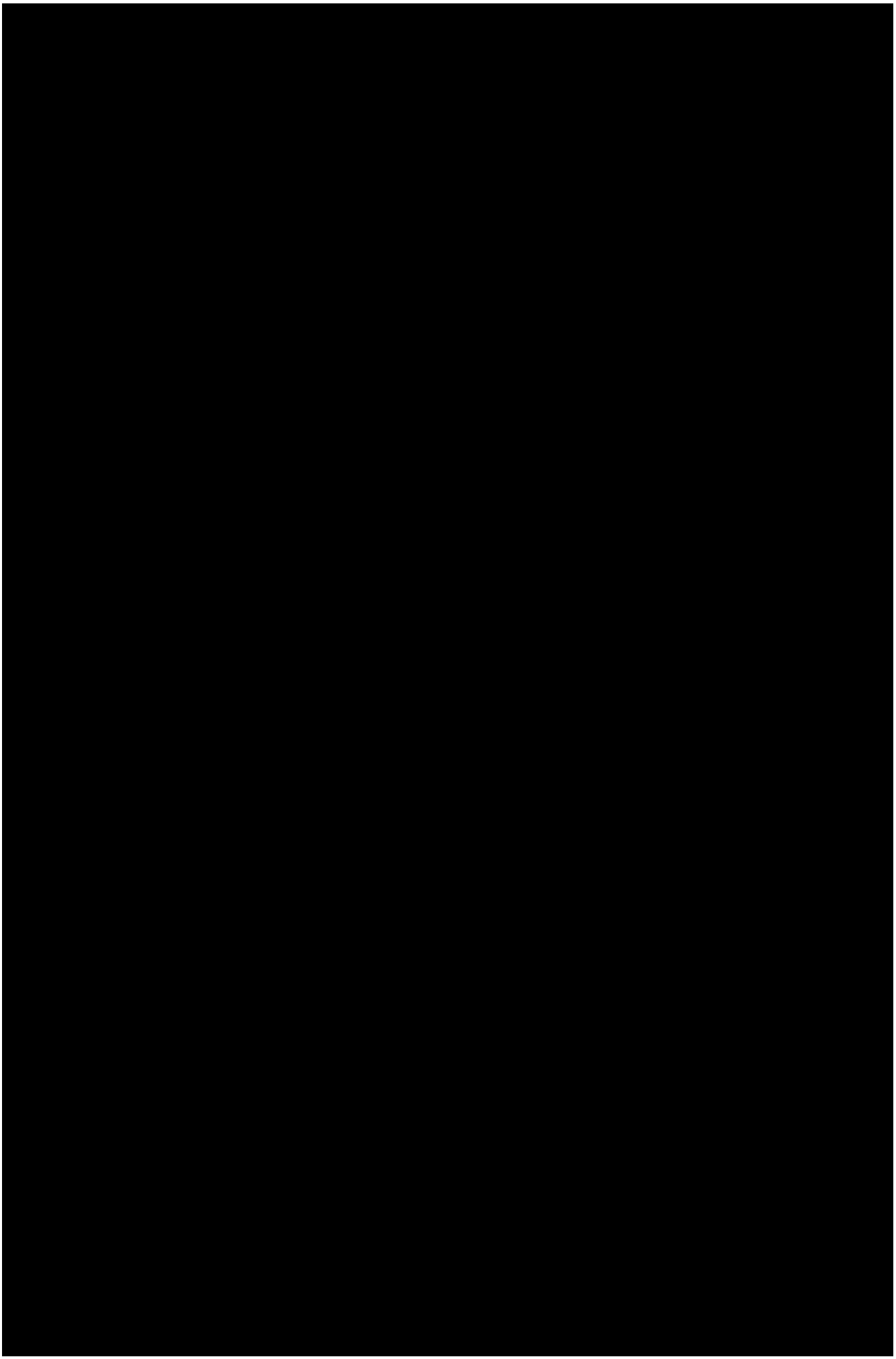
[Han18] Hanssen, Geir Kjetil; Dr. Stålhane, Tor; Myklebust, Thor (2018): SafeScrum® – Agile Development of Safety-Critical Software, Springer International Publishing.

[Mar08] Martin, Robert C. (2008): Clean Code: A Handbook of Agile Software Craftsmanship, Prentice Hall PTR.

Signatures

Number of pages (including this one): 116

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.



Signatures

Number of pages (including this one): 3

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

Verhaltenskodex für Lieferanten

Einführung

Die Deutsche Telekom AG und ihre verbundenen Unternehmen („DTAG“) handeln in Übereinstimmung mit ihrem

- „Code of Conduct“,
- Der menschenrechtlichen Grundsatzerklärung “Menschenrechtskodex” beides abrufbar unter dem Link https://www.telekom.com/de/verantwortung/details/menschenrechte-349790 sowie
- Leitlinien für Künstliche Intelligenz (KI-Leitlinien) abrufbar unter dem Link https://www.telekom.com/de/konzern/digitale-verantwortung.

Auf der Grundlage dieser Leitwerte, die sich auf Geschäftsethik, sowie menschenrechtliche und umweltbezogene Verpflichtungen beziehen, fordert die DTAG vom Lieferanten die Einhaltung der im Nachstehenden aufgeführten „Grundsätze“, welche dem zwischen ihnen geschlossenen Vertrag („Vertrag“) beigefügt werden. Der Lieferant setzt diese Grundsätze über seine ganze Lieferkette hinweg um. Dieser Verhaltenskodex für Lieferanten soll nicht die Gesetze und Vorschriften in den Ländern ersetzen, in denen Lieferanten der DTAG tätig sind. Vielmehr dient er der Förderung und Einhaltung dieser Gesetze und Vorschriften sowie der Gewährleistung, dass sie gewissenhaft und wirksam eingehalten werden.

GRUNDSÄTZE

1. Wesentliche Vertragspflichten

Die Parteien vereinbaren, dass die Einhaltung dieses Verhaltenskodexes eine wesentliche Pflicht des Vertrages darstellt.

Der Lieferant bemüht sich angemessen, seine eigenen Lieferanten, seine Auftragnehmer und Unterauftragnehmer (im Folgenden als „Unterauftragnehmer“ bezeichnet) sowie seine verbundenen Unternehmen zur Einhaltung der Grundsätze dieses Verhaltenskodex zu verpflichten, sofern sie bei der Erbringung der vertraglich vereinbarten Leistungen Anwendung finden. Der Lieferant kann seine Unterauftragnehmer dabei auf die Einhaltung seines eigenen Verhaltenskodex verpflichten, soweit dieser inhaltlich den Grundsätzen dieses Verhaltenskodex entspricht.

2. Umgang mit nationalem und internationalem Recht

Neben der Einhaltung der in den nachstehenden Ziffern 3 bis 6 enthaltenen Bestimmungen beachtet der Lieferant stets alle geltenden Gesetze, behördlichen Vorschriften sowie die zwischen dem Lieferanten und der DTAG (den „Parteien“) vereinbarten vertraglichen Pflichten. Dies gilt auch für die Antikorruptionsgesetze in den USA (US Foreign Corrupt Practices Act) und im Vereinigten Königreich (UK Bribery Act), sofern anwendbar. Ferner hält sich der Lieferant an alle internationalen Wirtschaftssanktionen (einschließlich Embargos), darunter alle Sanktionen, die ggf. aufgrund einer gemäß Kapitel VII der UN-Charta vom UN-Sicherheitsrat verabschiedeten Resolution gelten, sowie alle von der Europäischen Union auferlegten Sanktionen.

3. Zugrundeliegende Grundsätze

Der Lieferant hält die international anerkannten Menschenrechte ein und vermeidet eine Mitwirkung an jeglicher Art von Menschenrechtsverletzungen. Grundlage hierfür bilden die im „Menschenrechtskodex“ der DTAG veröffentlichten Erwartungen an Lieferanten. Der Lieferant respektiert insbesondere die persönliche Würde, die Privatsphäre und die Rechte jedes einzelnen Menschen. Sklaverei in jeglicher Form ist verboten. Ferner hält der Lieferant alle von der Internationalen Arbeitsorganisation (International Labour Organization, ILO) verfassten Standards und Übereinkommen ein.

4. Menschenrechte und faire Arbeitspraktiken

Die DTAG erwartet vom Lieferanten, dass

(1) er alle Arbeitnehmergesetze des jeweiligen Landes einhält,

(2) er die Grundsätze der DTAG zur Achtung der in Ziffer 3 aufgeführten Menschenrechte teilt und in Übereinstimmung mit der Internationalen Menschenrechtscharta der Vereinten Nationen, den UN-Leitprinzipien für Wirtschaft und Menschenrechte, den Prinzipien des UN-Global Compact und den ILO-Kernarbeitsnormen Chancengleichheit am Arbeitsplatz schafft,

(3) er wirksame Maßnahmen zur Beseitigung von Menschenrechtsverletzungen jeglicher Art und Verstößen gegen faire Arbeitsbedingungen ergreift, einschließlich der Offenlegung solcher und potenzieller Verstöße und

(4) er bei der Untersuchung von mutmaßlichen oder tatsächlichen Verstößen gegen diese Prinzipien, Normen und Übereinkommen umfassend kooperiert.

4.1 Vereinigungsfreiheit und Recht auf Kollektivverhandlungen

Der Lieferant muss die Rechte seiner Beschäftigten auf Vereinigungsfreiheit, Kollektivverhandlungen und friedliche Versammlung respektieren, einschließlich des Rechts, solchen Aktivitäten fernzubleiben, und hält dabei jeweils geltende nationale Gesetze und Verantwortlichkeiten sowie internationale Standards wie die Normen der Internationalen Arbeitsorganisation ein, je nachdem, welche Regelung strenger ist. Beschäftigte dürfen nicht eingeschüchtert, belästigt oder Repressalien ausgesetzt werden, wenn sie eines dieser Rechte in Anspruch nehmen. Werden diese Rechte durch nationale Gesetze oder Umstände eingeschränkt, sucht der Lieferant auf andere Weise den Dialog mit seinen Beschäftigten, um Fragen zu Beschäftigungsverhältnis und Probleme am Arbeitsplatz zu klären.

4.2 Kinderarbeit

Kinderarbeit darf in keiner Weise eingesetzt oder unterstützt werden und ist unter allen Umständen verboten. Die DTAG geht keine Geschäftsbeziehungen mit Lieferanten ein, die gegen diese Pflichten zur Verhinderung von Kinderarbeit direkt oder indirekt verstoßen. Der Lieferant ist dazu verpflichtet, insbesondere die beiden grundlegenden ILO-Übereinkommen über Kinderarbeit, Übereinkommen Nr. 138 über das Mindestalter und Übereinkommen Nr. 182 über die schlimmsten Formen der Kinderarbeit, einzuhalten. Der Lieferant darf niemanden beschäftigen, der jünger als 15 Jahre ist, noch schulpflichtig ist oder das gesetzliche Mindestalter für ein Beschäftigungsverhältnis nicht erreicht hat, wobei die Regelung mit der strengsten Altersgrenze Vorrang hat. Der Lieferant ist zur Einrichtung eines Maßnahmenplans verpflichtet, der bei Aufdeckung eines Falls von Kinderarbeit sicherstellt, dass der Lieferant Abhilfe schaffen muss und internationalen Standards oder Anforderungen nationaler Gesetze unverzüglich Folge leistet. Die DTAG unterstützt alle Formen der gesetzlich zulässigen Beschäftigung Jugendlicher, einschließlich der Entwicklung zulässiger Programme zur Ausbildung am Arbeitsplatz zugunsten der Bildung junger Menschen. Der Lieferant muss Beschäftigten unter 18 Jahren Tätigkeiten untersagen, die ihre Gesundheit oder Sicherheit gefährden, z. B. Nachtarbeit, Überstunden, schweres Heben und die Arbeit mit giftigen oder gefährlichen Stoffen.

4.3 Diversity und Gleichbehandlung

Der Lieferant untersagt und bekämpft direkte oder indirekte Diskriminierung wegen ethnischer Herkunft, der Hautfarbe, des Geschlechts, der sexuellen Orientierung, Sprache, Religion oder Glaubens, politischer oder anderer Anschauungen, nationaler oder sozialer Herkunft, der Vermögenslage, der Geburt, des Alters, Gesundheitszustands, einer Behinderung oder anderer Gründe und fördert Vielfalt, Chancengleichheit und Gleichbehandlung in Beschäftigung und Beruf. Darunter fällt auch die Zahlung ungleicher Entgelte für gleichwertige Arbeit. Der Lieferant behandelt alle Mitarbeiter respektvoll und wendet weder körperliche Züchtigung, psychischen oder physischen Zwang noch irgendeine Form von Missbrauch, Belästigung oder Androhung solcher Maßnahmen an.

4.4 Vergütung und Verbot der Zwangsarbeit

Der Lieferant bietet allen Angestellten und Arbeitern eine angemessene Vergütung, einschließlich solchen Beschäftigten, die dauerhaft oder vorübergehend beschäftigt werden, eine Behinderung haben oder Leiharbeiter, Zuwanderer, Auszubildende oder freie Mitarbeiter sind. Die Vergütung muss das laut nationaler Gesetze geltende Minimum erfüllen und dem branchenüblichen Niveau entsprechen. Gibt es keine entsprechenden gesetzlichen Standards in dem jeweiligen Land, so ist das Entgelt so zu bemessen, dass es die Grundbedürfnisse gemäß ILO-Übereinkommen Nr. 131 über die Festsetzung von Mindestlöhnen deckt. Den Arbeitskräften wird verständlich und zeitnah mitgeteilt, auf welcher Grundlage sie vergütet werden. Der Lieferant wendet keine Lohn- oder Gehaltskürzungen als Disziplinarmaßnahme an.

Der Lieferant beschäftigt niemanden, der zur Arbeit gezwungen wird. Dazu zählt jede Tätigkeit, die einer Person unter der Androhung von Strafe abverlangt wird oder für die sie sich nicht freiwillig zur Verfügung gestellt hat, z. B. infolge von Schuldknechtschaft oder Menschenhandel.

Der Lieferant verzichtet auf Sklaverei in jeglicher Form, der Sklaverei ähnliche Praktiken, Leibeigenschaft oder andere Formen der Herrschaft oder Unterdrückung am Arbeitsplatz, wie die extreme wirtschaftliche oder sexuelle Ausbeutung und Erniedrigung.

Der Lieferant darf zum Schutz seines Geschäfts keine privaten oder staatlichen Sicherheitskräfte einsetzen, wenn aufgrund mangelnder Einweisung oder Kontrolle durch den Lieferanten die Gefahr besteht, dass der Einsatz der Sicherheitskräfte gegen das Verbot der Folter und der grausamen, unmenschlichen oder erniedrigenden Behandlung verstößt oder eine Gefahr für Leib und Leben oder für die Vereinigungs- und Gewerkschaftsfreiheit darstellt.

4.5 Arbeitszeiten

Dem Lieferanten ist es untersagt, von Beschäftigten längere Arbeitszeiten zu verlangen, als es die gemäß internationaler Standards, einschließlich der Übereinkommen der Internationalen Arbeitsorganisation über übliche Arbeitszeiten (Übereinkommen Nr. 1, 14 und 106), nationaler Gesetze oder frei verhandelter und rechtmäßiger Kollektivverträge höchstens zulässige Stundenzahl erlaubt, wobei die strengere Regelung Vorrang hat. Der Lieferant muss sicherstellen, dass Überstunden freiwillig bzw. im Rahmen der gesetzlichen Vorgaben geleistet und unter Einhaltung nationaler Gesetze und Vorschriften vergütet werden. Eine Arbeitswoche darf einschließlich Überstunden nicht mehr

als 60 Arbeitsstunden umfassen, mit Ausnahme von Notfällen oder außergewöhnlichen Situationen. In einer Sieben-Tage-Arbeitswoche müssen Beschäftigte mindestens einen freien Tag haben dürfen. Der Lieferant muss unter Einhaltung nationaler Gesetze und Vorschriften Aufzeichnungen über die Arbeitsstunden seiner Beschäftigten und ihre Vergütung führen und diese Aufzeichnungen der DTAG auf Verlangen zur Verfügung stellen.

4.6 Arbeitsschutz

Der Lieferant ist zur Entwicklung und Umsetzung von Managementpraktiken für den Arbeitsschutz in allen Bereichen seiner Tätigkeit verpflichtet. Zu den Pflichten jedes Lieferanten gehören:

- Die Einhaltung und Umsetzung eines Prozesses, der sicherstellt, dass seine Beschäftigten alle geltenden Gesetze und Vorschriften über den betrieblichen Arbeitsschutz einhalten, einschließlich regelmäßiger Schulungen zu betrieblichem Arbeitsschutz, Notfallmaßnahmen, berufstypischen Verletzungen und Krankheiten, Hygiene im Betrieb, körperlich anspruchsvoller Arbeit, sicherer Maschinenbedienung, sanitärer Anlagen, Ernährung und Unterbringung.
- Die Bereitstellung einer sicheren Arbeitsumgebung für alle Beschäftigten, Maßnahmen zur Eindämmung arbeitsplatzbedingter Gefahrenquellen und die Umsetzung von Kontrollmechanismen zum Schutz verwundbarer Bevölkerungsgruppen.
- Die Schaffung eines Arbeitsschutzmanagementsystems (z. B. gemäß ISO 45001 oder gleichwertig), dass das Arbeitsschutzmanagement mindestens als integralen Bestandteil des Geschäfts erkennen lässt, das Führung ermöglicht und die Beschäftigten zur Mitgestaltung von Richtlinien, Rollen und Verantwortlichkeiten motiviert, das Risiken und Gefahren identifiziert und beurteilt und geeignete Kommunikationskanäle zur Information der Beschäftigten über Themen des Arbeitsschutzes bietet. Dieses Managementsystem muss Verfahren zur Erfassung und Untersuchung von Unfällen und Nachbesserungsmaßnahmen umfassen.
- Die kostenlose Bereitstellung geeigneter persönlicher Schutzausrüstung und die Einweisung der Beschäftigten in deren Gebrauch.
- Das Verbot des Konsums, Besitzes, Verkaufs oder der Verbreitung illegaler Drogen.

Der Ausstoß schädlicher Substanzen, mit denen am Arbeitsplatz umgegangen wird, wird so kontrolliert, dass die Konzentration die Grenzwerte der vor Ort geltenden Vorschriften zum Schutz der Belegschaft nicht überschritten wird oder falls es keine solchen Vorschriften gibt, nicht die Grenzwerte überschritten werden, oberhalb derer die Gesundheit langfristig gefährdet ist. Gleichermaßen muss Ausrüstung zur Verfügung stehen, die ein schnelles Vorgehen im Falle eines Austritts gefährlicher Substanzen, eines Brandes oder eines persönlichen Kontakts damit ermöglicht.

4.7 Beschwerdeverfahren

Der Lieferant muss seinen Beschäftigten in angemessener Weise wirksame Beschwerdeverfahren zur Verfügung stellen, damit sie ihre Probleme am Arbeitsplatz, einschließlich Belästigung und Diskriminierung, der Geschäftsführung zur Suche nach einer geeigneten Lösung melden können. Den Beschäftigten muss eine sichere Umgebung für Beschwerden und Feedback gegeben werden. Der Lieferant überprüft diese Meldeverfahren regelmäßig und muss den Lösungsfortschritt vorgebrachter Anschuldigungen oder Probleme in regelmäßigen Abständen überwachen.

Die Beschwerdeverfahren müssen zugänglich und kulturell angepasst sein und, soweit sinnvoll oder möglich, ein anonymes Meldeverfahren beinhalten. Beschäftigte oder ihre Vertreter müssen Ideen und Probleme bezüglich der Arbeitsbedingungen oder des Führungsstils offen kommunizieren und mit der Geschäftsleitung austauschen können, ohne Diskriminierung, Repressalien, Einschüchterungs-versuche oder Belästigung fürchten zu müssen. Der Lieferant muss die Beschäftigten regelmäßig über die Beschwerdeverfahren informieren und schulen. Jegliche Form der Vergeltung gegen Beschäftigte, die ein Problem am Arbeitsplatz melden, ist verboten. Der Lieferant übt keine Vergeltung durch persönliche Angriffe, Einschüchterungsversuche oder andere Drohungen gegen Beschäftigte aus, die Probleme am Arbeitsplatz melden wollen, einschließlich der Verletzung von Arbeitnehmerrechten, die sich aus nationalen Gesetzen oder internationalen Standards ergeben.

Ergänzend informiert der Lieferant seine Beschäftigten in angemessener Weise über die Nutzbarkeit des öffentlich verfügbaren Hinweisgeberportal „TellMe“ der DTAG: https://www.telekom.com/de/konzern/compliance/hinweisgeberportal

Soweit der Lieferant nicht über ein eigenes Beschwerdeverfahren verfügt, ist die Information über das Hinweisgeberportal „TellMe“ der DTAG ausreichend; die weiteren in dieser Ziffer festgelegten Grundsätze gelten hierfür entsprechend.

5. Ökologisch verantwortliches Handeln

5.1 Umweltschutz und Compliance

Die DTAG erkennt ihre soziale Verantwortung für den Umweltschutz an. Die DTAG erwartet von ihren Lieferanten, dass sie die Verpflichtung der DTAG gegen die Herausforderungen des Klimawandels teilen und einen Beitrag zum Umwelt- und Naturschutz und zum Erhalt der natürlichen Lebensgrundlage der Bevölkerung anstreben. Als Teil dieser Verpflichtung müssen alle Lieferanten:

- Alle geltenden Gesetze und Vorschriften des Umweltschutzes einhalten, einschließlich der Gesetze und Vorschriften über gefährliche Stoffe, Luft- und Wasseremissionen, schädliche Bodenveränderungen und Abfälle sowie gesetzliche Anforderungen und Branchenstandards, die die Verwendung bestimmter Substanzen in der Herstellung oder im Design von Produkten verbieten oder einschränken.

- Der Einhaltung aller vertraglichen Bestimmungen über die Kennzeichnung von Produkten und Verpackungen, wesentlicher Inhaltsstoffe, Recycling und Entsorgung zustimmen.
- Alle erforderlichen umweltrechtlichen Genehmigungen, regulatorischen Zustimmungen und Registrierungen einholen und aufrechterhalten.
- Alle Arten von Abfällen, darunter auch Wasser- und Energieverluste, vermeiden oder beseitigen, indem in den Einrichtungen des Lieferanten geeignete Einsparmaßnahmen ergriffen werden, und zwar (1) durch den Einsatz umweltfreundlicher Wartungs- und Produktionsverfahren und (2) durch die Umsetzung von Strategien zur Reduzierung, Wiederverwendung und Wiederverwertung von Stoffen (in dieser Reihenfolge), wann immer dies möglich ist und bevor sie entsorgt werden.
- Chemikalien, Abfälle oder andere Stoffe identifizieren, die freigesetzt werden könnten und möglicherweise eine Umweltgefahr darstellen, und mit solchen Chemikalien oder Stoffe so umgehen, dass die Sicherheit bei Handhabung, Transport, Lagerung, Verwendung, Wiederverwendung, Wiederverwertung und Entsorgung gewährleistet ist. Der Umgang mit ozonschädlichen Substanzen erfolgt in Übereinstimmung mit dem Montreal-Protokoll und geltenden Vorschriften.
- Vollständige, lückenlose, genaue und durch einen Dritten bestätigte Daten über die Treibhausgasemissionen (THG) nach Scope 1, 2 und 3 oder die zur Berechnung der THG-Emissionsdaten erforderlichen Variablen über das Carbon Disclosure Project (CDP) oder einen von der DTAG bereitgestellten alternativen Weg offenlegen. Auf Verlangen der DTAG muss der Lieferant Pläne zur Reduzierung der Treibhausgasemissionen in Übereinstimmung mit den Anforderungen der DTAG vorlegen.
- Die negativen Auswirkungen hinsichtlich Biodiversität, Entwaldung, Klimawandel und Wasserknappheit minimieren.
- Sicherstellen, dass die in der Herstellung von Produkten verwendeten Stoffe konfliktfrei sind und keinen Einfluss nehmen auf Konflikt- und Hochrisikogebiete im Sinne des OECD-Leitfadens für die Erfüllung der Sorgfaltspflicht zur Förderung verantwortungsvoller Lieferketten für Minerale, indem:
  - er seine Sorgfaltspflicht in der Beschaffungs- und Produktkette von Konfliktmineralien im Sinne des OECD-Leitfadens in seiner Lieferkette erfüllt und an einem etablierten Lieferketten-Kommunikationsprozess wie dem „Conflict-Free Smelter Program“ der Responsible Minerals Initiative teilnimmt oder einen national oder international anerkannten Lieferketten-Sorgfaltsstandard anwendet, z. B. den OECD-Leitfaden.
  - er der DTAG auf schriftliche Aufforderung alle Dokumente und Nachweise vorlegt, die die Maßnahmen des Lieferanten zur Erfüllung der Sorgfaltspflicht beweisen.

5.2 Natürliche Ressourcen und Abfallmanagement

Bei der Beschaffung oder Herstellung von Waren begrenzt der Lieferant den Material- und Ressourceneinsatz, um deren Umweltauswirkungen auf ein Mindestmaß zu beschränken.
Die Nutzung seltener Ressourcen ist zu begrenzen bzw. weitestgehend zu vermeiden. Die durch die gesamte Geschäftstätigkeit des Lieferanten erzeugten Abfälle sind zu identifizieren, zu kontrollieren und zu verwalten. Der Lieferant bemüht sich um eine Verringerung der Abfallmenge. Bei der Abfallentsorgung sind die geltenden Umweltschutzgesetze zu beachten.

5.3 Einsatz von Quecksilber

Der Lieferant verzichtet auf die Herstellung quecksilberhaltiger Produkte gemäß Artikel 4 Absatz 1 und Anhang A Teil I des Minamata-Übereinkommens. Der Lieferant verzichtet in seinem Herstellungsprozess gemäß Art. 5 Abs. 2 und Anhang B Teil I des Minamata-Übereinkommens nach dem vom Übereinkommen für die jeweiligen Produkte bzw. Prozesse vorgegebenen Ausstiegsdatum auf die Verwendung von Quecksilber und allen Quecksilberverbindungen. Der Lieferant verzichtet auf eine Handhabung von Quecksilberabfällen, die gegen die Bestimmungen von Art. 11 Abs. 3 des Minamata-Übereinkommens verstößt.

5.4 Handhabung persistenter organischer Schadstoffe

Der Lieferant verzichtet auf die Herstellung und Verwendung der in Art. 3 Abs. 1 Buchst. a) und Anhang A des Stockholmer Übereinkommens über persistente organische Schadstoffe (POP-Übereinkommen) aufgeführten Chemikalien, soweit geltendes nationales Recht dies in Übereinstimmung mit dem Stockholmer Übereinkommen regelt. Er verzichtet auch darauf, dass Abfälle in nicht umweltgerechter Weise entgegen der in Übereinstimmung mit Art. 6 Abs. 1 d) (i) und (ii) des POP-Übereinkommens geltenden gesetzlichen Vorschriften gehandhabt, gesammelt, befördert und gelagert werden.

6. Untersagte Geschäftspraktiken

6.1 Korruption

Der Lieferant unterlässt jede Art der Korruption sowie Handlungen, die als solche ausgelegt werden könnten.
Der Lieferant darf Amtsträgern bzw. privatwirtschaftlichen Entscheidern im In- und Ausland keine illegalen Vorteile anbieten, versprechen oder gewähren, um eine Bevorzugung oder eine günstige Entscheidung im öffentlichen oder privaten Sektor zu erwirken. Dies ist auch beim Umgang mit Spenden, Geschenken oder Einladungen zu Geschäftsessen und Veranstaltungen zu berücksichtigen.
Der Lieferant darf nicht zulassen, dass ihm Vorteile versprochen oder angeboten werden, und darf keine Vorteile in Anspruch nehmen, falls dies bei der die Vorteile gewährenden Person den Anschein erweckt oder erwecken kann, dass sie auf diese Weise die Geschäftsentscheidungen des Lieferanten beeinflussen

könnte. Entsprechend darf der Lieferant auch nicht die Gewährung von Vorteilen verlangen.
Der Lieferant vermeidet Interessenskonflikte, die Korruptionsrisiken mit sich bringen können.
Ist der Lieferant auch ein Kunde der DTAG, darf er aus diesem Umstand keine unbilligen Vorteile ziehen und hat Einkauf und Vertrieb streng zu trennen.
Der Lieferant verpflichtet sich zu Folgendem und verlangt dies von seinem Vorstand sowie seinen Führungskräften, Mitarbeitern, Lieferanten, verbundenen Unternehmen, Unterauftragnehmern und allen entsprechenden Vertretern (im Folgenden als „Dritte“ bezeichnet):

- die Vorschriften des vorliegenden Absatzes 5.1 sowie die Bestimmungen in Absatz 1 („die Vorschriften“) anhand geeigneter Mittel zur wirksamen Implementierung und Pflege eines Compliance-Systems einzuhalten;
- dass (i) alle an der Erfüllung des Vertrags beteiligten Dritten die Vorschriften einhalten und dass (ii) alle von den Dritten zur Erfüllung des Vertrags benötigten und angewandten Mittel den Vorschriften entsprechen.

6.2 Wettbewerb

Der Lieferant hält sich in jeder Geschäftsbeziehung an die Regeln des freien und fairen Wettbewerbs und verstößt insbesondere nicht gegen Wettbewerbs- und Kartellgesetze.

6.3 Sponsoring

Alle Sponsoringaktivitäten des Lieferanten müssen mit geltenden Gesetzen in Einklang stehen.

6.4 Politische Spenden

Der Lieferant tätigt Geldspenden an politische Parteien oder gewährt diesen geldwerte Vorteile ausschließlich im rechtlich zulässigen Rahmen.

6.5 Geldwäsche

Der Lieferant ergreift alle Maßnahmen zur Verhinderung von Geldwäsche in seinem Einflussbereich.

6.6 Datensicherheit, Datenschutz und KI-Leitlinien

Die Datenverarbeitungsprozesse und KI-Algorithmen, sowie die Datennutzung sind nachvollziehbar zu dokumentieren, der DTAG bei Bedarf offenzulegen und unterliegen geltenden Gesetzen und Vorschriften, insbesondere den gesetzlichen und den konkreten in diesem Vertrag vereinbarten Datenschutz- und Sicherheitsbestimmungen. Die Entwicklung und Anwendung von Künstlicher Intelligenz erfolgt nach den europäischen Grundwerten. Der Einsatz von KI-Systemen ist gegenüber den Nutzern diskriminierungsfrei und transparent zu gestalten.
Ein barrierefreier Zugang wird gewährleistet.

Der Lieferant hat für seine KI-Lösungen klar definiert, wer für welches System und welche KI-Funktion verantwortlich ist und schafft die Voraussetzungen, seine KI-Systeme jederzeit durch den verantwortlichen Anwender anzuhalten oder abzuschalten („Not-Aus-Schalter“).

Der Lieferant hält alle geltenden Datenschutzgesetze sowie alle konkreten, in diesem Vertrag vereinbarten Datenschutz- und Datensicherheitsbestimmungen ein.

7. Compliance-Audits und Abhilfemaßnahmen

7.1 Audits und Abhilfemaßnahmen

Um die Einhaltung der in diesem Verhaltenskodex für Lieferanten festgelegten Grundsätze während der Vertragslaufzeit sicherzustellen, stellt der Lieferant auf Verlangen alle für die Feststellung der Einhaltung dieser Grundsätze angeforderten Mittel zur Verfügung und informiert die DTAG unverzüglich, sobald er Kenntnis oder eine begründete Vermutung dahingehend hat, dass er selbst oder ein Unterauftragnehmer die Grundsätze nicht eingehalten hat. Diese Information umfasst auch die bereits zur Wiederherstellung der Einhaltung der Grundsätze getroffenen Korrekturmaßnahmen. Des Weiteren stellt der Lieferant unverzüglich alle Informationen zur Verfügung, die zur Einhaltung der geltenden Vorschriften erforderlich sind.
Im Falle einer Änderung der gesetzlichen bzw. regulatorischen Rahmenbedingungen sowie bei juristischen Entscheidungen, die eine Verletzung der Grundsätze durch eine der Parteien mit sich bringen würde, kann die DTAG einschlägige Änderungen vornehmen, die der Lieferant befolgen muss.
Falls im Vertrag nicht festgelegt, gilt für geschäftsethische, menschenrechtliche und/oder umweltbezogen und Compliance-Audits folgendes: Die DTAG bzw. ihr bevollmächtigter Vertreter ist berechtigt, Bewertungs- und Monitoring-Maßnahmen beim Lieferanten und dessen Unterauftragnehmern durchzuführen, um die tatsächliche Einhaltung der Grundsätze durch den Lieferanten und dessen Unterauftragnehmer effektiv zu beurteilen. Dies umfasst das Recht der DTAG bzw. ihres bevollmächtigten Vertreters, Audits durchzuführen, u. a. Beurteilungen und Inspektionen vor Ort, Befragungen sowie Gespräche mit ausgewählten Beschäftigten auf dem Gelände, an Produktionsstandorten oder anderen Standorten des Lieferanten, an denen im Auftrag der DTAG oder in Zusammenhang mit von der DTAG eingekauften Produkten und Dienstleistungen Arbeiten ausgeführt werden. Der Lieferant erkennt an, dass die DTAG das Recht hat, weitere Informationen über Belange der gesellschaftlichen Verantwortung von Unternehmen (CSR) oder Nachhaltigkeit mittels Selbstauskünften des Lieferanten (z. B. EcoVadis/Carbon Disclosure Project/Umfragen über mobile Endgeräte) anzufordern und zu erhalten, falls dies für notwendig erachtet wird. Auf Verlangen der DTAG gibt der Lieferant Auskunft über zur Sicherstellung der Einhaltung der Grundsätze ergriffenen Maßnahmen. Im Falle von Verstößen gegen die Grundsätze ist die DTAG über jeden einzelnen Verstoß in Kenntnis zu setzen; anschließend ist ein konkreter Verbesserungsplan

vorzulegen und zeitnah umzusetzen. Falls die DTAG bestimmt, dass der Verstoß nicht in angemessener Zeit und unverzüglich beseitigt werden kann, hat die DTAG das Recht ein Konzept zu erstellen und umzusetzen, das potenzielle Risiken minimiert und konkrete Maßnahmen, Verantwortlichkeiten und Meilensteine vorsieht. Zu diesem Zweck kann die DTAG insbesondere mit anderen Unternehmen zusammenarbeiten und die Geschäftsbeziehung während der Maßnahmen zur Risikominimierung bei Bedarf aussetzen. Die DTAG begrenzt jeglichen Zugriff auf Geschäftsgeheimnisse des Lieferanten während ihrer Beurteilungen und Inspektionen auf das Nötigste und macht von diesen Geheimnissen allenfalls Gebrauch, um die Einhaltung der in diesem Dokument festgelegten Grundsätze zu überprüfen. Ein wesentlicher Verstoß gegen die Grundsätze kann ein Recht auf Kündigung des Vertrags gemäß seinen Bestimmungen nach sich ziehen.

7.2 Nachhaltigkeitstraining

Die DTAG bietet allen externen Geschäftspartnern und Lieferanten Nachhaltigkeitstrainings an. Der Lieferant muss sicherstellen, dass seine Beschäftigten und Unterauftragnehmer, die an Belangen der DTAG arbeiten, die Anforderungen des Verhaltenskodex für Lieferanten kennen, beispielsweise durch geeignete Schulungen zu den Regelungen und Grundsätzen dieses Vertrags.

Signatures

Number of pages (including this one): 7

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

Allgemeine Geschäftsbedingungen der Deutschen Telekom Gruppe für den Einkauf von ICT-Dienstleistungen (EB ICT Services)

1. Geltungsbereich

(1) Diese Einkaufsbedingungen der Deutschen Telekom Gruppe für den Einkauf von ICT-Dienstleistungen (im Folgenden als EB ICT Services bezeichnet) gelten für alle Dienstleistungen im Bereich der ICT-Dienstleistungen (im Folgenden als Dienstleistungen bezeichnet), die der Auftragnehmer (jede Person oder Firma, die Dienstleistungen unter Bezugnahme auf diese Bedingungen erbringt) der Deutschen Telekom AG (im Folgenden als DTAG bezeichnet) oder einem mit der Deutschen Telekom AG verbundenen Unternehmen (jedes verbundene Unternehmen gemäß §§ 15 ff. AktG sowie jedes Unternehmen weltweit, an dem die DTAG direkt oder indirekt mindestens 25 Prozent der Anteile hält oder eine gleichwertige Managementkontrolle ausübt) erbringt, sofern die Bestellung keine abweichenden Bedingungen enthält. Die bestellende Konzerngesellschaft wird im Folgenden als „Auftraggeber“ bezeichnet.

(2) Der Auftragnehmer bietet dem Auftraggeber Dienstleistungen gemäß den Spezifikationen dieser Einkaufsbedingungen für ICT-Dienstleistungen unter Bezugnahme auf dieselben an. Vereinbarungen über die Dienstleistungen des Auftragnehmers (im Folgenden als „Bestellungen“ bezeichnet) werden durch eine Bestellung unter Bezugnahme auf ein entsprechendes Angebot des Auftragnehmers getroffen.

(3) Art und Inhalt der Dienstleistungen werden in der jeweiligen Bestellung definiert und detailliert beschrieben.

(4) Nur Bestellungen und andere Willenserklärungen, die schriftlich vom Auftraggeber abgegeben werden, sind rechtsverbindlich. Bestellungen erfolgen ohne Kauf- oder Abrufverpflichtung; etwaige angegebene Mengen sind lediglich Schätzungen und der Auftragnehmer hat keinen Anspruch auf den Abruf oder die Bestellung der gesamten Menge. Die Schriftformerfordernis wird auch durch E-Mail oder speziell vom Auftraggeber bereitgestellte elektronische Kommunikationsmethoden zur Durchführung von Einkaufsprozessen, einschließlich vollständig integrierter, webbasierter Anwendungen oder über das Order Management Tool übermittelte Erklärungen, erfüllt. Eine elektronische Willenserklärung gilt an dem Tag als zugegangen, an dem sie während der normalen Geschäftszeiten unter der elektronischen Adresse des Empfängers abrufbar ist; andernfalls gilt sie am nächsten Geschäftstag als zugegangen. Sofern der Auftraggeber eine spezielle elektronische Kommunikationsmethode bereitstellt, gelten die entsprechenden Nutzungsbedingungen der Deutschen Telekom Gruppe („NB e-commerce“) (siehe unter https://www.telekom.com/de/konzern/einkauf).

2. Bestandteile des Vertrags

(1) Die folgenden Unterlagen werden mit Vertragsschluss mit abnehmender Priorität Teil des Vertrags:

a. Die Bestellung
b. Andere in der Bestellung spezifizierte Vertragsbestandteile, z.B. aber nicht beschränkt auf Leistungsbeschreibungen, Projektvereinbarungen und Angebote
c. Der Rahmenvertrag (falls vorhanden)
d. Diese EB ICT Services
e. Der „DTAG Supplier Code of Conduct“ in seiner jeweils aktuellen Fassung (im Folgenden als „Code of Conduct“ oder „ScoC“ bezeichnet; siehe https://www.telekom.com/de/konzern/einkauf).

(2) Allgemeine Geschäftsbedingungen des Auftragnehmers finden keine Anwendung, auch wenn sie im Angebot oder anderen Dokumenten des Auftragnehmers erwähnt werden oder auf sie Bezug genommen wird und der Auftraggeber ihnen nicht ausdrücklich widerspricht. Es gibt und wird keine mündlichen Ergänzungen zu diesem Vertrag oder einer Bestellung geben.

(3) Zur Vermeidung von Missverständnissen: Die Bestellung und alle anderen Vertragsbestandteile definieren nur die Details der vertraglichen Leistung des Lieferanten und legen die jeweiligen kommerziellen Bedingungen fest. Wenn die Parteien von den in diesem Vertrag festgelegten rechtlichen Bestimmungen abweichen wollen, müssen sie ausdrücklich auf den Abschnitt verweisen, den sie im jeweiligen Dokument ändern oder ersetzen wollen. Ein ausdrücklicher Verweis ist nicht erforderlich, wenn die Änderung wegen zwingenden lokalen Rechts erfolgt.

(4) Werden die vorgenannten Formalitäten nicht eingehalten gelten abweichende Bestimmungen als ungültig und die Bestimmungen dieses Vertrags bleiben unverändert, es sei denn, die Parteien vereinbaren innerhalb von fünf (5) Geschäftstagen nach Feststellung einer solchen Unstimmigkeit schriftlich etwas anderes.

3. Allgemeine Rechte und Pflichten der Parteien

(1) Der Auftragnehmer verpflichtet sich selbst, alle Unterauftragnehmer, Unterlieferanten und jede Person unter seiner Kontrolle zur Einhaltung des DTAG Supplier Code of Conduct zu verpflichten, der unter https://www.telekom.com/de/konzern/einkauf verfügbar ist. Der Auftragnehmer ergreift alle erforderlichen Maßnahmen, um jede Form von aktiver oder passiver Korruption sowohl im öffentlichen als auch im privaten Sektor zu vermeiden und zu sanktionieren. Der Auftragnehmer garantiert, dass die Dienstleistungen zum Lieferdatum oder – je nach Fall – ab dem vereinbarten Bereitstellungsdatum allen geltenden Gesetzen, Vorschriften, Verordnungen, Richtlinien und Anordnungen („Gesetze“) entsprechen. Der Auftragnehmer garantiert ferner, alle Registrierungs- und Meldepflichten gegenüber den jeweiligen Regierungsbehörden zu übernehmen und alle diesbezüglichen anfallenden Gebühren rechtzeitig zu zahlen. Der Auftragnehmer garantiert auch, dem Auftraggeber alle notwendigen Informationen zur Verfügung zu stellen, um dem Auftraggeber die Erfüllung aller Verpflichtungen zu ermöglichen, die für den Auftraggeber als (Wieder-)Verkäufer oder Vertreiber der Dienstleistungen gelten können.

(2) Der Auftragnehmer verpflichtet sich, den Auftraggeber unverzüglich schriftlich zu benachrichtigen, sobald ihm Probleme im Zusammenhang mit der Einhaltung des Supplier Code of Conduct in seinem Verantwortungsbereich bekannt werden, und insbesondere alles zu vermeiden, was das Markenimage der Deutschen Telekom Gruppe schädigen oder die zuverlässige Erbringung der Dienstleistungen gefährden könnte.

(3) Der Auftragnehmer ist verpflichtet, die Sicherheitsbestimmungen der Deutschen Telekom Gruppe (siehe: https://www.telekom.com/de/konzern/einkauf) einzuhalten, die für den Auftragnehmer und seine Erfüllungsgehilfen gelten. Der Auftragnehmer informiert die zur Leistungserbringung eingesetzten Personen und/oder Unterauftragnehmer darüber und verpflichtet sie ebenfalls zur Einhaltung der Sicherheitsbestimmungen.

(4) Wenn Arbeiten an sicherheitssensiblen Standorten des Auftraggebers durchgeführt werden sollen, stellt der Auftragnehmer sicher, dass nur Mitarbeiter eingesetzt werden, die in Deutschland gemäß dem Sicherheitsüberprüfungsgesetz oder anderorts gemäß einem vergleichbaren Sicherheitsstandard eine Sicherheitsüberprüfung bestanden haben.

(5) Der Auftragnehmer stellt sicher, dass sowohl er als auch seine Unterauftragnehmer die gesetzlichen Bestimmungen der jeweils geltenden Mindestlohngesetzgebung (z.B. das deutsche „Mindestlohngesetz“) einhalten. In diesem Zusammenhang sind sie beispielsweise verpflichtet, auf Verlangen des Auftraggebers schriftlich nachzuweisen, dass der Mindestlohn von ihnen und ihren Unterauftragnehmern gezahlt wird. Der Auftragnehmer stellt den Auftraggeber von allen Ansprüchen im Zusammenhang mit Mindestlohnzahlungen frei, einschließlich etwaiger verhängter Bußgelder. Er informiert den Auftraggeber auch unverzüglich, wenn es Anhaltspunkte dafür gibt, dass er oder einer seiner Unterauftragnehmer gegen die gesetzlichen Mindestlohnanforderungen verstößt oder verstoßen hat.

(6) Der Auftragnehmer hält die Anforderungen des Auftraggebers an Qualitätsmanagement, Umweltschutz und Informationssicherheit ein. Soweit dies in einer Spezifikation gefordert wird, (i) weist der Auftragnehmer ein Qualitätsmanagement gemäß DIN EN ISO 9001, TL 9000 oder einem gleichwertigen Qualitätsmanagementsystem nach und stellt Daten zu den im TL 9000 Quality Management System Measurements Handbook beschriebenen Kennzahlen oder einer anderweitig vereinbarten Kennzahl zur Verfügung, (ii) weist der Auftragnehmer ein Umweltmanagementsystem gemäß DIN EN ISO 14001 oder dem Eco-Management and Audit Scheme nach und (iii) weist der Auftragnehmer ein Informationssicherheitsmanagementsystem gemäß ISO/IEC 27001 oder einem gleichwertigen System nach.

(7) Der Auftragnehmer führt genaue Aufzeichnungen über alle Angelegenheiten, die sich auf seine Verpflichtungen hierunter beziehen, gemäß den allgemein anerkannten Rechnungslegungsgrundsätzen und -praktiken, einheitlich und konsistent angewendet, in einem Format, das eine unkomplizierte Prüfung ermöglicht. Der Auftragnehmer bewahrt diese Aufzeichnungen für einen Zeitraum von zehn (10) Jahren ab dem Datum der endgültigen Zahlung unter der Bestellung, auf die sich diese Aufzeichnungen beziehen, auf. Soweit diese Aufzeichnungen relevant sein können, um festzustellen, ob der Auftragnehmer seine Verpflichtungen aus der jeweiligen Bestellung erfüllt, haben DTAG, die bestellende Partei und deren autorisierte Vertreter während der normalen Geschäftszeiten angemessenen Zugang zu diesen Aufzeichnungen zur Einsichtnahme und Prüfung. Der Auftragnehmer wird alle zumutbaren Hilfestellungen im Zusammenhang mit einer Prüfung leisten.

(8) Auftraggeber und Auftragnehmer benennen Ansprechpartner mit Entscheidungsbefugnis, um die fach- und termingerechte Ausführung der Bestellungen sicherzustellen.

(9) Der Auftragnehmer ist verpflichtet, die Einkaufsbereiche des Auftraggebers unverzüglich und unaufgefordert zu informieren, wenn der Auftragnehmer oder von ihm zur Erbringung der vertraglichen Leistungen eingesetztes Personal (Mitarbeiter oder Unterauftragnehmer) gleichzeitig in anderen parallelen Projekten innerhalb der Deutschen Telekom Gruppe während des Einsatzzeitraums beschäftigt ist oder eine solche Beschäftigung geplant ist. Sollte der Auftragnehmer dieser Informationspflicht nicht nachkommen, behält sich der Auftraggeber ausdrücklich das Recht vor, eine Prüfung aller Zahlungen zu veranlassen, die von Einheiten der Deutschen Telekom Gruppe für solche parallellaufenden Projekte geleistet wurden, und die in diesem Zusammenhang geleisteten Zahlungen zurückzufordern.

4. Leistung

(1) Der Auftragnehmer wird nur entsprechend qualifiziertes Personal zur Erfüllung der vertraglichen Verpflichtungen einsetzen. Auf Anforderung im jeweiligen Angebot wird der Auftragnehmer dem Auftraggeber eine Beschreibung der Ausbildung und Arbeitsprofile der eingesetzten oder einzusetzenden Mitarbeiter vorlegen, die deren Qualifikation für die zu erbringende Leistung nachweist.

(2) Der Auftragnehmer stellt sicher, dass seine Leistungen mit der üblichen beruflichen Sorgfalt erbracht werden, dass sie auf dem Stand der Wissenschaft und Technik basieren und dass sie allen relevanten gesetzlichen Bestimmungen und den vereinbarten Richtlinien entsprechen.

(3) Geringfügige Mängel werden unverzüglich behoben, sofern keine neue Leistung erforderlich ist.

(4) Der Auftraggeber ist ausdrücklich berechtigt, die Nachbesserung des Lieferanten innerhalb einer vom Auftraggeber festgelegten angemessenen Frist zu verlangen und die Vergütung für die Erbringung der ICT-Dienstleistung entsprechend zu mindern, wenn die Nachbesserung verzögert wird oder nach Ablauf der Nachfrist fehlschlägt.

(5) Alle weiteren Rechte des Auftraggebers, die ihm gesetzlich oder vertraglich zustehen, bleiben unberührt.

(6) Sofern gesetzlich keine längeren Fristen vorgesehen sind, verjähren die Ansprüche des Auftraggebers wegen Rechtsmängeln innerhalb von zwei Jahren ab dem Zeitpunkt, in dem ein Dritter einen Anspruch wegen Verletzung gewerblicher Schutzrechte oder sonstiger Rechte geltend macht oder der Auftraggeber auf andere Weise von dem Rechtsmangel Kenntnis erlangt.

(7) Die vorbehaltlose Zahlung des Rechnungsbetrages durch den Auftraggeber stellt keine Anerkennung der Leistung des Auftragnehmers als vertragsgemäß dar. Die Anerkennung der Leistungen oder Teilleistungen erfolgt durch den Auftraggeber nur, wenn der Lieferant seine ICT-Dienstleistungen gemäß der Bestellung oder einer anderen zwischen den Parteien vereinbarten Spezifikation erbracht hat.

5. Unabhängige Leistungserbringung

(1) Der Auftragnehmer erbringt die vertraglichen Leistungen eigenverantwortlich und selbstständig.

(2) Grundsätzlich ist der Auftragnehmer frei in der Wahl des Erfüllungsortes für die Erbringung seiner Leistungen. Erfordert das Projekt jedoch eine teilweise Erbringung der Leistungen auf dem Gelände des Auftraggebers oder eines Dritten, so ist der Auftragnehmer bereit, die Leistungen in dem erforderlichen Umfang an den jeweiligen Standorten zu erbringen; die Parteien werden den jeweiligen Erfüllungsort unter Berücksichtigung der Projektanforderungen gesondert vereinbaren.

(3) Der Auftragnehmer ist allein verantwortlich für die Erteilung von Anweisungen an seine Mitarbeiter und die von ihm eingesetzten Subunternehmer. Der Auftragnehmer ist frei in der Organisation der Leistungserbringung und der Zeiteinteilung für seine Tätigkeiten. Soweit es das Projekt erfordert, koordiniert sich der Auftragnehmer jedoch mit den anderen am Projekt Beteiligten, um die vereinbarten Termine einzuhalten.

(4) Der Auftragnehmer verpflichtet sich, die vom Auftraggeber erhaltene Vergütung eigenständig und ordnungsgemäß gemäß den einschlägigen Steuergesetzen zu versteuern.

(5) Setzt der Auftragnehmer Mitarbeiter, Erfüllungsgehilfen und Subunternehmer ein, stellt er sicher, dass alle dafür erforderlichen behördlichen Genehmigungen (z.B. Arbeits- und Aufenthaltserlaubnis) vorliegen. Der Auftragnehmer stellt den Auftraggeber von allen rechtlichen Konsequenzen frei, die sich aus der Nichteinhaltung dieser Anforderung ergeben.

(6) Der Auftraggeber stellt dem Auftragnehmer (soweit zur Leistungserbringung erforderlich) alle ihm zur Verfügung stehenden Informationen und Unterlagen zur Verfügung.

(7) Der Auftragnehmer ist verpflichtet, den Auftraggeber jederzeit über den Stand der Arbeiten zu informieren.

(8) Erkennt der Auftragnehmer, dass er die vereinbarten Fertigstellungstermine nicht einhalten kann, so hat er den Auftraggeber unverzüglich schriftlich über die Gründe und die Dauer der voraussichtlichen Verzögerung zu informieren. Ein Anspruch auf Verlängerung der Fertigstellungstermine besteht nicht. Die gesetzlichen und vertraglichen Folgen einer Verzögerung bleiben unberührt.

(9) Der Auftragnehmer ist voll verantwortlich für den Einsatz und die Leistung seines Personals im Zusammenhang mit der Leistungserbringung. Bei Arbeiten auf dem Gelände des Auftraggebers ist der Auftragnehmer verpflichtet sicherzustellen, dass sein Personal das Eigentum des Auftraggebers sorgfältig behandelt.

(10) Das mit der Erbringung der betreffenden Leistungen betraute Personal muss die im Zusammenhang mit der jeweiligen Bestellung festgelegten Qualifikationen besitzen. Ein neuer Mitarbeiter des Auftragnehmers muss in der Regel mindestens die gleichen Qualifikationen wie der vorherige (ersetzte) Mitarbeiter haben. Höhere Kosten, die mit einem Wechsel der Mitarbeiter (z.B. Einarbeitung / projektspezifische Wissensvermittlung) verbunden sind, trägt der Auftragnehmer.

(11) Der Einsatz von Mitarbeitern des Auftragnehmers in Projekten mit Wettbewerbern der Deutschen Telekom Gruppe bedarf der schriftlichen Zustimmung des Auftraggebers, wenn diese Mitarbeiter gleichzeitig in Projekten für den Auftraggeber tätig sind oder in den letzten 6 Monaten in solchen Projekten eingesetzt waren.

(12) Erbringt der Auftragnehmer Leistungen für Endkundenprojekte der DTAG oder eines verbundenen Unternehmens im Sinne von § 1 (1), verpflichtet sich der Auftragnehmer während der Laufzeit des jeweiligen Auftrags und für ein Jahr nach dessen Beendigung nicht in vergleichbarer Weise für die jeweiligen Endkunden zu arbeiten, es sei denn, der Auftraggeber erteilt eine schriftliche Zustimmung zu einer solchen Tätigkeit. Diese Zustimmung darf nicht unbillig verweigert werden. Die vorstehende Verpflichtung des Auftragnehmers gilt nur, wenn und soweit die Endkunden in der Bestellung für die jeweilige Leistung bereits benannt sind.

6. Preisgestaltung

(1) Der im Vertrag vereinbarte Preis ist entweder ein Festpreis oder, im Falle einer Vergütung auf Zeit- und Materialbasis, ein Höchstpreis (Gesamtnettopreis).

(2) Die vereinbarte Vergütung deckt alle im Zusammenhang mit der Leistungserbringung anfallenden Kosten ab, insbesondere die Leistungen von Subunternehmern, alle Nebenkosten, Reisekosten sowie Reise- und Wartezeiten, sofern in der jeweiligen Bestellung nicht anders angegeben.

(3) Der Auftragnehmer stellt sicher, dass die DTAG und ihren verbundenen Unternehmen angebotenen Preise für die Leistungen die Preise, die vergleichbaren Dritten innerhalb Europas (oder der jeweiligen Region) gewährt werden, nicht übersteigen. Hat der Auftraggeber berechtigte Zweifel an der Einhaltung dieser Verpflichtung durch den Auftragnehmer, ist der Auftraggeber berechtigt, die Einhaltung dieser Verpflichtung durch einen unabhängigen Dritten, der der beruflichen Schweigepflicht unterliegt, überprüfen zu lassen. Der Auftragnehmer unterstützt den Dritten bei der Überprüfung und gewährt Zugang zu allen erforderlichen Informationen und Unterlagen. Stellt die Überprüfung fest, dass der Auftragnehmer seine Verpflichtung nicht einhält, übernimmt der Auftragnehmer die Kosten der Überprüfung und erstattet dem Auftraggeber den bis zur Preisänderung zu viel gezahlten Betrag unverzüglich zurück und passt die Preise mit sofortiger Wirkung entsprechend an.

(4) Zusätzliche Leistungen, die während der Laufzeit eines Vertrages erforderlich werden und Kosten verursachen, sind von den Parteien schriftlich zu vereinbaren, bevor sie erbracht werden, auch wenn sie für die Erfüllung des Vertrages unerlässlich sind.

7. Rechnungsstellung und Zahlungsbedingungen

(1) Die Rechnungsstellung erfolgt nach vollständiger Leistungserbringung, sofern die Parteien nicht schriftlich etwas anderes vereinbart haben.

(2) Wurde eine Vergütung auf Zeit- und Materialbasis vereinbart, erfolgt die Rechnungsstellung in der Regel monatlich gemäß einem vom Auftraggeber festgelegten Leistungs-protokollierungsverfahren. Ist kein elektronisches Leistungsprotokollierungssystem verfügbar, ist der Rechnung ein im Original unterschriebener Leistungsnachweis beizufügen, sofern die Parteien nichts anderes vereinbart haben. Die Rechnung kann ohne Bearbeitung zurückgewiesen werden, wenn dieser Leistungsnachweis nicht beigefügt ist. Gleiches gilt bei Preisabweichungen, falschen Angaben zu Bestellpositionen oder fehlender Bestellnummer (SAP-Nummer). Bei der Rechnungsstellung auf Zeit- und Materialbasis muss der Rechnungsmonat auf der Rechnung angegeben werden.

(3) Rechnungen sind ausschließlich an die in der Bestellung angegebene Rechnungsadresse zu senden.

(4) Die Rechnung wird nicht vor Leistungserbringung bezahlt. Sofern in der Bestellung nichts anderes vereinbart ist, beträgt die Zahlungsfrist 30 Tage netto. Die Zahlungsfrist beginnt am ersten Tag nach Eingang einer prüffähigen Rechnung, die den

Anforderungen dieses Abschnitts 7 entspricht, jedoch nicht vor Leistungserbringung.

(5) Die Rechnung muss den Anforderungen des § 14 des deutschen Umsatzsteuergesetzes (UStG) entsprechen. Entspricht die Rechnung nicht den Anforderungen, behält sich der Auftraggeber das Recht vor, die ausstehende Rechnung zur Vervollständigung oder Korrektur zurückzusenden. In einem solchen Fall beginnt die Zahlungsfrist erst nach Eingang einer vervollständigten oder korrigierten Rechnung. Auch wenn der Auftraggeber von dem vorgenannten Vorbehalt keinen Gebrauch macht, ist er nicht für eine durch solche Fehler verursachte Zahlungsverzögerung verantwortlich. Die Rechnung darf frühestens an dem Tag ausgestellt werden, an dem die Leistung gemäß dem Vertrag erbracht wurde.

(6) Änderungen und Ergänzungen des Auftrags sind in der Rechnung deutlich zu kennzeichnen und werden nur bezahlt, wenn sie vor ihrer Ausführung schriftlich vereinbart wurden.

(7) Wurde ein Gutschriftverfahren vereinbart, gelten abweichend von oder zusätzlich zu den Bestimmungen dieses Abschnitts 7 die folgenden Bestimmungen:

Der Auftraggeber wird Zahlungen leisten, ohne dass der Auftragnehmer Rechnungen einreichen muss. Die Zahlungsfrist beginnt mit Abschluss der Dateneingabe, jedoch nicht vor Erbringung/Abnahme der Leistung. Die Leistung wird auf Basis eines Leistungsnachweises abgerechnet. Der Auftragnehmer erhält vom Auftraggeber monatlich am 3. Arbeitstag des Folgemonats einen Gutschriftbericht als Nachweis der elektronisch erfassten Leistungen. Der Gutschriftbericht listet die Leistungen nach Art und Menge sowie den Nettopreis, die Mehrwertsteuer und den Mehrwertsteuersatz für jeden Leistungsnachweis auf.
Im Übrigen gelten die Bestimmungen dieses Abschnitts 7.

8. Steuern

(1) Der Auftragnehmer verpflichtet sich, die vom Auftraggeber erhaltene Vergütung eigenständig und ordnungsgemäß unter Einhaltung aller relevanten Steuergesetze zu versteuern.

(2) Alle Steuern, Zölle, Abgaben und sonstigen fiskalischen Belastungen im Zusammenhang mit dem Abschluss und der Durchführung dieses Vertrags trägt der Auftragnehmer, mit Ausnahme der Mehrwertsteuer und vergleichbarer Verbrauchssteuern wie Waren- und Umsatzsteuern oder Nutzungs- und Umsatzsteuern.

(3) Alle Preise sind Nettopreise ohne Mehrwertsteuer und vergleichbare Verbrauchssteuern. Jegliche Mehrwertsteuer oder vergleichbare Verbrauchssteuern wie Waren- und Umsatzsteuern oder Nutzungs- und Umsatzsteuern trägt der Auftraggeber. Sollten solche Steuern zu zahlen sein, stellt der Auftragnehmer diese dem Auftraggeber in Rechnung und hält sich dabei stets an die jeweils geltenden Steuergesetze zur Ausweisung der Steuern in der Rechnung. Soweit die Steuerschuld für die vorgenannten Steuern aufgrund einer gesetzlichen Bestimmung auf den Auftraggeber als Empfänger der Vertragsleistungen übergeht, darf der Auftragnehmer keine Steuern in seiner Rechnung ausweisen oder berechnen.

(4) Der Auftraggeber zahlt keine Einkommen-, Körperschafts- oder sonstigen vergleichbaren Steuern des Auftragnehmers, die im Zusammenhang mit dem Abschluss und der Durchführung dieses Vertrags stehen. Soweit nach deutschem oder einem anderen Einkommen- oder Körperschaftssteuergesetz Quellensteuern fällig werden, ist der Auftraggeber berechtigt, den gesetzlich vorgeschriebenen Mindestbetrag der Steuer von den vereinbarten Zahlungen einzubehalten. Wenn es zulässig ist, die Quellensteuer in einem solchen Fall ganz oder teilweise aufgrund eines Doppelbesteuerungsabkommens zu reduzieren, wird der Auftragnehmer, falls zutreffend, die erforderlichen Unterlagen oder amtlichen Bescheinigungen dem Auftraggeber vorlegen, damit der Auftraggeber im Rahmen der gesetzlichen Bestimmungen ganz oder teilweise auf den Abzug der Quellensteuer verzichten kann. Der Auftraggeber wird den Auftragnehmer in diesem Zusammenhang in zumutbarem Umfang unterstützen.

(5) Ungeachtet des Vorstehenden, falls Quellensteuern nicht vermeidbar sind und falls Steuern einbehalten wurden, wird der Auftraggeber dem Auftragnehmer die Steuerbescheinigungen, die die Höhe der einbehaltenen Steuern belegen, rechtzeitig nach Zahlung der Steuern an die zuständigen Steuerbehörden zur Verfügung stellen.

9. Außenhandelsvorschriften

(1) Die vom Auftragnehmer zu erbringenden Leistungen können europäischen, deutschen, US-amerikanischen oder anderen nationalen Gesetzen und Vorschriften unterliegen. Der Auftragnehmer ist dafür verantwortlich, die Einhaltung aller anwendbaren Vorschriften im Zusammenhang mit der Erbringung der Leistungen sicherzustellen.

(2) Der Auftragnehmer verpflichtet sich, alle gemäß den Exportvorschriften erforderlichen Genehmigungen für die grenzüberschreitende Erbringung von Leistungen eigenverantwortlich und auf eigene Kosten einzuholen und alle relevanten Gesetze und Vorschriften einzuhalten.

(3) Falls der Auftragnehmer Leistungen ganz oder teilweise von Dritten bezogen hat, garantiert er, dass diese aus sicheren Quellen stammen und unter Beachtung und Einhaltung aller Export- und sonstigen relevanten gesetzlichen Vorschriften des Herstellungs-/Versandlandes exportiert, importiert oder bereitgestellt wurden.

(4) Darüber hinaus verpflichtet sich der Auftragnehmer bei der Durchführung des Vertrags insbesondere zur Einhaltung der europäischen Gesetzgebung, des deutschen Außenwirtschaftsrechts und des US-amerikanischen Re-Exportrechts.

10. Verzug

(1) Im Falle des Verzugs gelten die gesetzlichen Bestimmungen, sofern nachstehend nichts anderes bestimmt ist.

(2) Der Auftraggeber gerät nur in Verzug, wenn er nach einer schriftlichen Mahnung des Auftragnehmers eine Zahlung nicht leistet.

(3) Falls eine Vertragsstrafe vereinbart wurde, kann der Auftraggeber sich das Recht vorbehalten, die Vertragsstrafe bis zur endgültigen Zahlung geltend zu machen.

11. Nutzungsrechte

(1) Liefert der Auftragnehmer Arbeitsergebnisse (neue Produkte und andere Ergebnisse, die mit der Erbringung der vertraglich vereinbarten Leistungen zusammenhängen) im Rahmen eines Auftrags (erstellt durch den Auftragnehmer, dessen Mitarbeiter oder Subunternehmer bei der Erbringung der ICT-Dienstleistungen), gewährt der Auftragnehmer dem Auftraggeber ein unwiderrufliches, übertragbares, ausschließliches Nutzungsrecht für alle Nutzungsarten das inhaltlich, zeitlich und geografisch

unbeschränkt ist, einschließlich des Quellcodes (falls zutreffend) und der Dokumentation. Die gewährten Rechte umfassen uneingeschränkt die Nutzung, Vermarktung, Veränderung oder sonstige kommerzielle Verwertung der Arbeitsergebnisse durch den Auftraggeber, insbesondere das Recht zur Vervielfältigung, Verbreitung, Ausstellung, Vorführung und Aufführung sowie das Recht zur Reproduktion mittels Bild- und Tonträgern.
Falls es entstanden ist, wird das Nutzungsrecht an jedem einzelnen Arbeitsergebnis dem Auftraggeber am Ende des Arbeitstages des Auftragnehmers eingeräumt. Das Nutzungsrecht wird dem Auftraggeber spätestens an dem Tag eingeräumt, an dem die vereinbarte Tätigkeit endet. Die vorgenannte Einräumung der Nutzungsrechte gilt auch insoweit, als die Art der Nutzung zum Zeitpunkt des Abschlusses des Auftrags noch nicht bekannt ist.

(2) Hinsichtlich bestehender Produkte (integriert in die Arbeitsergebnisse oder anderweitig erforderlich zur Nutzung der Arbeitsergebnisse) oder Standardsoftware (falls vorhanden) einschließlich der entsprechenden Dokumentation gewährt der Auftragnehmer dem Auftraggeber ein einfaches Nutzungsrecht für alle Nutzungsarten das inhaltlich, zeitlich und geografisch unbeschränkt ist, übertragbar innerhalb der DTAG-Gruppe, zur internen Nutzung und zur Leistungserbringung gegenüber den Kunden der DTAG-Gruppe, zu denen auch alle Personen gehören, die für die DTAG-Gruppe in den Räumlichkeiten der DTAG-Gruppe arbeiten. Darüber hinaus kann der Auftraggeber jederzeit weitere Lizenzen mit den gleichen Nutzungsrechten erwerben.
Der Auftragnehmer wird den Auftraggeber im Voraus über solche bestehenden Produkte informieren.

(3) Der Auftraggeber ist berechtigt, aber nicht verpflichtet, die Werke zu nutzen und zu verwerten. Darüber hinaus ist der Auftraggeber berechtigt, aber nicht verpflichtet, den Urheber der Werke auf oder im Zusammenhang mit den Werken zu nennen.

(4) Sofern nicht schriftlich anders vereinbart sind alle Gebühren, für die dem Auftraggeber gemäß diesem Abschnitt 11 gewährten Rechte, in der in der jeweiligen Bestellung vereinbarten Vergütung enthalten.

12. Rechte Dritter

(1) Der Auftragnehmer garantiert, dass:
- (i) die Vertragsleistungen keine Rechte Dritter, insbes. Schutzrechte und Rechte des geistigen Eigentums, verletzen und dass keine solchen Rechte die Nutzung der Vertragsleistungen gemäß diesem Vertrag und den jeweiligen Aufträgen verhindern werden;
- (ii) keine zusätzlichen Lizenzen, Genehmigungen oder Zustimmungen in Bezug auf solche Rechte an geistigem Eigentum (einschließlich Zahlungen an Verwertungsgesellschaften) für den Auftraggeber, seine verbundenen Unternehmen und Kunden erforderlich sind, soweit dies für die Nutzung der Vertragsleistungen gemäß diesem Vertrag und den jeweiligen Aufträgen erforderlich ist; und
- (iii) der Urheber der in die Vertragsleistungen eingebetteten Rechte an geistigem Eigentum seine Urheberpersönlichkeitsrechte, soweit dies nach den jeweiligen Gesetzen möglich ist, nicht geltend machen wird, z.B. sein Recht auf Zugang oder Nennung als Urheber.

(2) Der Auftragnehmer wird den Auftraggeber (einschließlich seiner Vertreter, Mitarbeiter und Beauftragten) vollständig von allen Klagen, Ansprüchen, Schäden (einschließlich Verlusten) und Aufwendungen (einschließlich Kosten und Gebühren) freistellen, die aus allen Handlungen und Forderungen resultieren, die dem Auftraggeber aufgrund einer Verletzung oder angeblichen Verletzung von Rechten an geistigem Eigentum Dritter oder einer der oben genannten Garantien entstehen oder entstehen könnten.
Zur Klarstellung: Eine solche Verletzung oder angebliche Verletzung umfasst:
- (i) jede indirekte und/oder beitragsabhängige Verletzung; und
- (ii) jede Handlung der Verletzung und/oder angeblichen Verletzung nach dem Grundsatz der gemeinsamen unerlaubten Handlung.

Im Falle einer beitragsabhängigen Verletzung ist der Auftragnehmer anteilig entsprechend seinem Beitrag zur Verletzung verantwortlich.

(3) Der Auftragnehmer hat keine Haftung oder Verpflichtung zur Freistellung des Auftraggebers in Bezug auf Ansprüche Dritter wegen Verletzung, wenn die Verletzung ausschließlich verursacht wurde durch:
- (i) eine Änderung der Vertragsleistungen durch den Auftraggeber ohne Zustimmung des Auftragnehmers; oder
- (ii) die Kombination der Vertragsleistungen mit anderen Produkten, die nicht in der Spezifikation aufgeführt sind und die für den Auftragnehmer im Hinblick auf die beabsichtigte Nutzung der Vertragsleistungen nicht vorhersehbar ist.

(4) Jede Partei wird die andere Partei unverzüglich über jegliche Ansprüche Dritter bezüglich der Rechte an geistigem Eigentum informieren, die gegen die andere Partei geltend gemacht oder angedroht werden und/oder wenn sie Kenntnis von einer Verletzung oder potenziellen Verletzung von Rechten an geistigem Eigentum Dritter in den vertraglichen Leistungen erlangt. Die Parteien werden versuchen, so bald wie möglich eine gemeinsame Verteidigungsvereinbarung ("GVV") bezüglich des Anspruchs abzuschließen, sobald sie von solchen Ansprüchen Kenntnis erlangen. Diese GVV soll das Recht des Auftraggebers beinhalten, Zugang zu vertraulichen Prozessinformationen zu haben, die einer Schutzanordnung der Gerichte unterliegen, falls vorhanden, sowie zu allen anderen Informationen im Zusammenhang mit dem Anspruch. Der Auftraggeber wird dem Auftragnehmer (a) die alleinige Kontrolle und Autorität über die Verteidigung in Bezug auf die vertraglichen Lieferungen mit DTAG und/oder dem Auftraggeber gewähren, wobei der Auftraggeber berechtigt ist, auf Kosten des Auftragnehmers an der Verteidigung teilzunehmen; und (b) alle verfügbaren Informationen, Unterstützung und Autorität zur Verfügung stellen, die vernünftigerweise notwendig sind, um einen solchen Anspruch oder eine solche Klage zu verteidigen. Ungeachtet des Vorstehenden werden sowohl der Auftragnehmer als auch der Auftraggeber alle Anstrengungen unternehmen, um den Schaden für den Auftraggeber so weit wie möglich gemäß § 254 II BGB zu mindern.

(5) Wenn die Nutzung der vertraglichen Lieferungen oder Teile davon durch eine Gerichtsentscheidung untersagt wird oder wenn nach vernünftiger Einschätzung des Auftragnehmers eine Klage wegen Verletzung von Rechten an geistigem Eigentum unmittelbar bevorsteht oder eingereicht wurde, wird der Auftragnehmer – zusätzlich zu seinen anderen Verpflichtungen gemäß dieses Abschnitts 12 – nach eigenem Ermessen und auf eigene Kosten entweder:
- (i) solche vertraglichen Lieferungen oder Teile davon ändern oder ersetzen, um die Verletzung oder angebliche Verletzung der Rechte an geistigem Eigentum Dritter zu vermeiden, jedoch so, dass die

geänderten oder ersetzten Lieferungen in jeder Hinsicht den Spezifikationen und anderen Anforderungen dieser Vereinbarung und der Bestellung in Bezug auf die vertraglichen Lieferungen entsprechen; oder

(ii) dem Auftraggeber das Recht verschaffen, die vertraglichen Lieferungen wie in dieser Vereinbarung und der jeweiligen Bestellung vorgesehen weiter zu nutzen.

Falls ein Anspruch oder eine Information (z.B. ein Schreiben das auf bestimmte Patente hinweist) auf einem Standard-Essential-Patent oder einem angeblichen Standard-Essential-Patent beruht, wird der Auftragnehmer alle angemessenen Maßnahmen ergreifen, um DTAG und den/die Auftraggeber gegen den Anspruch oder die Information des Dritten zu verteidigen (einschließlich, aber nicht beschränkt auf die Bereiterklärung, eine Lizenz zu erwerben, ein Lizenzangebot zu machen, die Nichtverletzung oder Erschöpfung des Patents geltend zu machen oder eine Nichtigkeitsklage zu erheben), um alle Rechte von und für DTAG und ihre verbundenen Unternehmen für alle Länder, in denen DTAG und ihre verbundenen Unternehmen tätig sind, vollständig zu wahren, einschließlich, aber nicht beschränkt auf alle notwendigen Schritte, um zu verhindern, dass der Dritte in der Lage ist, eine einstweilige Verfügung oder ein ähnliches Rechtsmittel zu beantragen, wobei alle rechtlichen Anforderungen erfüllt werden, die vernünftigerweise vom Auftragnehmer erwartet werden können, um dieses Ziel zu erreichen. "Standard-Essential-Patent" bedeutet Patente, die für die Herstellung, Nutzung und den Verkauf der vertraglichen Lieferungen, die den formalen technischen Standards entsprechen, wie sie von international anerkannten Normungsorganisationen (wie GSMA, ETSI, DIN usw.) festgelegt wurden, unerlässlich sind. Der Auftragnehmer ist insbesondere verpflichtet – falls zutreffend – (i) dem anspruchstellenden Dritten ein Angebot zu unterbreiten, das den Grundsätzen der Entscheidung des Europäischen Gerichtshofs mit der Aktennummer C-170/13 (Huawei gegen ZTE) und allen nachfolgenden Entscheidungen dazu gemäß der Praxis und Rechtsprechung der zuständigen nationalen Gerichte entspricht und das in Gerichtsverfahren verwendet werden kann (falls rechtlich notwendig im Namen von DTAG oder dem Auftraggeber), oder (ii) eine Klage gegen diesen Dritten zu erheben, um solche Lizenzen zu erhalten.

Falls der Auftragnehmer nicht in der Lage ist, alle notwendigen Lizenzen für Standard-Essential-Patente (auf denen der Anspruch basiert) innerhalb des durch die Praxis und Rechtsprechung des jeweiligen Gerichts erforderlichen Zeitraums, jedoch in jedem Fall innerhalb von höchstens sechs Monaten nach Erhalt der Benachrichtigung über den Anspruch gemäß Unterabschnitt 4 oben zu erhalten, haben DTAG und/oder der Auftraggeber das Recht, auf Kosten des Auftragnehmers zu versuchen, diese Lizenzen direkt vom Dritten zu FRAND-Bedingungen (fair, angemessen und nicht diskriminierend) zu erhalten, und der Auftragnehmer wird DTAG oder den Auftraggeber, je nach Fall, für solche gezahlten FRAND-Lizenzgebühren entschädigen; der Auftraggeber – unter Beachtung der Vertraulichkeitsbestimmungen – wird den Auftragnehmer über die Lizenzbedingungen informieren. Wenn der Auftragnehmer die Lizenzgebühr nicht als FRAND betrachtet, ist der Auftragnehmer berechtigt zu beweisen, dass eine niedrigere Lizenzgebühr den FRAND-Bedingungen entspricht; in einem solchen Fall wird der Auftragnehmer nur den nachgewiesenen FRAND-Betrag der Lizenzgebühr zahlen, und falls der Auftragnehmer bereits den vollen Betrag gezahlt hat, wird der nicht-FRAND-Teil der Lizenzgebühr dem Auftragnehmer erstattet.

Zur Vermeidung von Missverständnissen gilt dieser Unterabschnitt 5 auch in Fällen von einstweiligen Verfügungen und Grenzbeschlagnahmen, die von Dritten initiiert wurden.

(6) Falls der Auftragnehmer es versäumt, die Verletzung der Rechte an geistigem Eigentum Dritter durch die Umsetzung der Alternativen (i) oder (ii) des Unterabschnitts 5 oben oder – unter den oben genannten Bedingungen – durch den Erwerb aller notwendigen Lizenzen im Falle von Standard-Essential-Patenten innerhalb eines von DTAG und/oder dem Auftraggeber festgelegten angemessenen Zeitraums zu beenden, ist der Auftraggeber berechtigt, nach eigenem Ermessen die jeweilige Bestellung zu widerrufen und entsprechend Schadensersatz zu verlangen.

(7) Lieferantenverpflichtung

Der Auftragnehmer verpflichtet sich hiermit unwiderruflich gegenüber DTAG und den verbundenen Unternehmen, ohne Zahlung einer zusätzlichen Gebühr oder Lizenzgebühr, keine rechtlichen Schritte gegen DTAG und ihre verbundenen Unternehmen in Bezug auf Produkte und Dienstleistungen einzuleiten, die von einem Dritten (einschließlich, aber nicht beschränkt auf Wettbewerber des Auftragnehmers) an DTAG oder seine verbundenen Unternehmen geliefert werden und die der Auftragnehmer als Verletzung der Rechte des Lieferanten an geistigem Eigentum betrachtet ("Verpflichtung, nicht zu klagen").

Dieses Instrument ist eine Verpflichtung, nicht zu klagen, und keine Freigabe. Dem Auftragnehmer steht es weiterhin frei, gegen einen solchen Dritten vorzugehen und vor den Gerichten alle notwendigen Rechtsmittel zu suchen und alle Arten von rechtlichen Schritten einzuleiten, um die Verletzung zu vermeiden und/oder aufzuhalten, auch wenn solche Schritte zu einer Gerichtsentscheidung führen würden, die das Geschäft von DTAG und seinen verbundenen Unternehmen betrifft.

Die Verpflichtung, nicht zu klagen, gilt auch für alle vertraglichen Lieferungen, die vom Auftragnehmer an DTAG oder eines ihrer verbundenen Unternehmen geliefert oder bereitgestellt wurden, falls der Auftragnehmer nach der Lieferung oder Bereitstellung solcher vertraglichen Lieferungen Rechte an geistigem Eigentum, die mit den vertraglichen Lieferungen in Zusammenhang stehen, an einen Dritten (einschließlich, aber nicht beschränkt auf eine nicht-praktizierende Einheit) abgetreten, verkauft, vermietet, belastet, lizenziert, unterlizenziert oder anderweitig übertragen oder gewährt hat.

Falls der Auftragnehmer der Ansicht ist, dass Produkte von DTAG oder eines verbundenen Unternehmens, die von DTAG/einem verbundenen Unternehmen oder auf Geheiß von DTAG/einem verbundenen Unternehmen entwickelt wurden, die Rechte des geistigen Eigentums des Auftragnehmers verletzen, werden die Parteien zunächst darüber verhandeln und alle Anstrengungen unternehmen, um diese Angelegenheit einvernehmlich zu regeln, bevor sie gerichtliche Schritte einleiten. Der Auftragnehmer wird davon absehen, einstweiligen Rechtsschutz gegen DTAG oder ein verbundenes Unternehmen zu suchen.

Diese Verpflichtung, nicht zu klagen, ist bindend für den Auftragnehmer, seine Rechtsnachfolger und Nachfolger im Titel solcher Rechte an geistigem Eigentum, Abtretungsempfänger und Testamentsvollstrecker, Verwalter und persönliche Vertreter.

Für den Fall, dass der Auftragnehmer nach dem Inkrafttreten dieser Vereinbarung Rechte an geistigem Eigentum an einen Dritten abtritt, verkauft, vermietet, belastet, lizenziert, unterlizenziert oder anderweitig überträgt oder gewährt, garantiert der Auftragnehmer, dass dieser Dritte an die

Verpflichtung, nicht zu klagen, in der gleichen Weise gebunden ist, wie in diesem Abschnitt dargelegt.

(8) Haftung, Verjährung
Die in dieser Vereinbarung festgelegten Haftungsbeschränkungen gelten nicht für diesen Abschnitt. Alle Ansprüche, die diesem Abschnitt unterliegen, verjähren gemäß den gesetzlichen Bestimmungen zwei Jahre nach dem Zeitpunkt, zu dem DTAG und der Auftraggeber positive Kenntnis von einem solchen Anspruch erlangt haben.

13. Subunternehmer

(1) Die Beauftragung eines Subunternehmers (einschließlich externer Berater und Freiberufler) bedarf der schriftlichen Zustimmung des Auftraggebers; eine solche Zustimmung kann ohne Angabe von Gründen verweigert werden. Der Auftragnehmer muss bevorzugte Subunternehmer durch Angabe ihres Namens, ihrer Firmendaten und ihres Beschäftigungsstatus im Angebot angeben. Verbundene Unternehmen des Auftragnehmers gelten gemäß diesem Abschnitt 13 als Subunternehmer.

(2) Falls der Auftragnehmer einen Subunternehmer beschäftigen möchte, muss der Auftragnehmer seine Marge in diesem Zusammenhang in seinem Angebot angeben. Im Falle einer Untervergabe ohne Zustimmung des Auftraggebers ist der Auftraggeber berechtigt, die vereinbarte Vergütung um die Marge des Auftragnehmers zu kürzen.

(3) Zur Vermeidung von Missverständnissen darf die Zustimmung des Auftraggebers zur Untervergabe keinesfalls als Erlaubnis für den jeweiligen Unterauftragnehmer ausgelegt werden, weitere Untervergaben in seinem Namen zu arrangieren. Jede weitere Untervergabe bedarf der ausdrücklichen schriftlichen Zustimmung des Auftraggebers. Darüber hinaus gelten die Bestimmungen dieses Abschnitts 13 entsprechend für jede weitere Untervergabe – insbesondere so, dass die Marge und die vertragliche Transparenz sowie das Verbot von Wettbewerbsbeschränkungen die gesamte Kette der Untervergabe abdecken müssen. Eingesetzte Berater, die weder Mitarbeiter noch Angestellte des Auftragnehmers oder eines Unterauftragnehmers sind („Freelancer“) und die vorübergehend eingestellt werden, gelten ebenfalls als Unterauftragnehmer im Sinne dieser EB ICT Services und erweitern die gleiche Kette. Dieser Status des Beraters ist im Angebot anzugeben.

(4) Eine Bestellung stellt keinen Arbeitsvertrag zwischen dem Auftraggeber und einer Person dar, die vom Auftragnehmer oder einem Unterauftragnehmer beschäftigt wird. Der Auftragnehmer und seine Unterauftragnehmer sind für alle Arbeitgeberpflichten verantwortlich, die ihnen aufgrund öffentlicher Vorschriften, durch eine Behörde aufgrund öffentlicher Vorschriften oder durch eine Behörde infolge der Ausführung eines Auftrags und in Bezug auf das zu versteuernde Einkommen des Auftragnehmers auferlegt werden. Darüber hinaus haftet der Auftraggeber nicht für Gehälter, Reisekosten, persönliche Steuern, Sozialversicherungsbeiträge und Versicherungsprämien usw. in Bezug auf Mitarbeiter oder Berater des Auftragnehmers oder deren Unterauftragnehmer. Der Auftragnehmer stellt den Auftraggeber von jeglicher Haftung frei und hält den Auftraggeber schadlos von jeglichen Handlungen oder Unterlassungen, die gegen diese Verpflichtung verstoßen.

(5) Wenn der Auftraggeber seine Zustimmung zur Untervergabe erteilt, stellt der Auftragnehmer sicher, dass alle im Rahmen des jeweiligen Auftrags vergebenen Unteraufträge so organisiert sind, dass der Auftragnehmer in vollem Umfang in der Lage ist, seine Verpflichtungen gegenüber dem Auftraggeber zu erfüllen.

(6) Der Auftragnehmer legt dem Auftraggeber zur Information seine Standardverträge vor, die er mit seinen Unterauftragnehmern verwendet. In jedem Fall darf der Auftragnehmer keine Vereinbarungen mit seinen Unterauftragnehmern abschließen, die den Unterauftragnehmern verbieten, nach Abschluss der Untervergabebeziehung eine Vereinbarung, entweder direkt oder indirekt, mit dem Auftraggeber abzuschließen.

(7) Die Haftung des Auftragnehmers bleibt von der Untervergabe, von den Informationen über die Struktur der Untervergabebeziehung oder von der Zustimmung des Auftraggebers dazu unberührt.

(8) Der Auftraggeber ist berechtigt, die Richtigkeit der vom Auftragnehmer in der jeweiligen Einzelbestellung angegebenen Margen durch direkten Kontakt mit dem Unterauftragnehmer zu überprüfen. In diesem Zusammenhang verpflichtet sich der Auftragnehmer, den Unterauftragnehmer in dem erforderlichen Umfang von seinen Vertraulichkeitsverpflichtungen zu entbinden. Der Auftragnehmer legt auf Anfrage des Auftraggebers die Vereinbarung mit dem Unterauftragnehmer zur stichprobenartigen Überprüfung der oben genannten Margen offen.

14. Vertraulichkeit, Datenschutz

(1) Beide Parteien verpflichten sich hiermit, alle Informationen der anderen Partei, die ihnen durch ihre Geschäftsbeziehung bekannt werden und die nicht allgemein zugänglich sind, vertraulich zu behandeln; solche Informationen dürfen nicht für eigene oder fremde Zwecke verwendet werden. Diese Verpflichtung zur Vertraulichkeit gilt nicht innerhalb der Deutschen Telekom Gruppe.

(2) Wenn die Offenlegung vertraulicher Informationen durch Regel, Gericht, Gesetz, Staat, Behörde oder zuständiger politischer Untergliederung verlangt wird, muss die empfangende Partei (a) die offenlegende Partei so weit wie rechtlich möglich und sobald sie davon Kenntnis hat, dass eine solche Offenlegung erforderlich ist, informieren und (b) der offenlegenden Partei die Möglichkeit geben, die Notwendigkeit einer solchen Offenlegung zu überprüfen und zu genehmigen oder rechtliche Schritte zu unternehmen, um die Offenlegung zu verhindern. In keinem Fall stellt die Offenlegung vertraulicher Informationen an eine fordernde Behörde wie oben beschrieben einen Verstoß gegen die Vertraulichkeitsverpflichtung gemäß dieser Vereinbarung dar. Darüber hinaus ist die offenlegende Partei in keiner Weise für die Nutzung der vertraulichen Informationen durch die fordernde Behörde wie oben beschrieben verantwortlich.

(3) Die empfangende Partei darf die vertraulichen Informationen ohne vorherige schriftliche Zustimmung der offenlegenden Partei nicht an Dritte weitergeben und muss die vertraulichen Informationen unter Sicherheitsbedingungen aufbewahren, die nicht weniger streng sind als die für vertrauliche Informationen der empfangenden Partei von vergleichbarer Sensibilität, und in jedem Fall angemessene Vorsichtsmaßnahmen für deren sichere Verwahrung treffen. Verbundene Unternehmen gelten in diesem Zusammenhang nicht als Dritte, müssen jedoch dennoch die Vertraulichkeit wie hier vereinbart wahren. Die Parteien haben das Recht, vertrauliche Informationen auf einer Need-to-know-Basis an ihre Mitarbeiter, Vertreter, Auftragnehmer, Berater und verbundenen Unternehmen des Lieferanten weiterzugeben, wenn die jeweilige Partei, die die vertraulichen Informationen weitergibt, eine Vereinbarung mit den vorgenannten Personen abgeschlossen hat, die Vertraulichkeitsbestimmungen enthält, die denen hierin

entsprechen, und auf Anfrage der anderen Partei einen Nachweis darüber erbringt. Die Partei, die die vertraulichen Informationen wie oben beschrieben weitergibt, haftet gegenüber der anderen Partei für jeden Verstoß gegen die Vertraulichkeitsverpflichtungen durch eine der vorgenannten Personen, einschließlich ihrer verbundenen Unternehmen.

(4) Der Auftragnehmer verpflichtet sich, das Fernmeldegeheimnis zu wahren und gewährleistet dem Auftraggeber, dass er seine Verpflichtungen gemäß allen anwendbaren Datenschutzgesetzen, insbesondere der DSGVO, ordnungsgemäß erfüllt.

(5) Alle dem Auftragnehmer vom Auftraggeber zur Leistungserbringung zur Verfügung gestellten Unterlagen bleiben Eigentum des Auftraggebers und sind auf Verlangen des Auftraggebers vom Auftragnehmer zurückzugeben oder zu vernichten, zusammen mit allen angefertigten Kopien. Duplikate von Dokumenten in elektronischen Medien und auf Datenträgern, die nicht übergeben werden können, müssen vom Auftragnehmer gelöscht oder dauerhaft unbrauchbar gemacht werden. Dies gilt auch im Falle der Beendigung dieser Vereinbarung. Der Auftragnehmer hat kein Zurückbehaltungsrecht, unabhängig von den rechtlichen Gründen.

(6) Der Auftragnehmer verpflichtet sich, seine Mitarbeiter, Vertreter und Unterauftragnehmer ausdrücklich und nachweislich darüber zu informieren, dass der Auftraggeber die folgenden personenbezogenen Daten über sie zum Zwecke der Einhaltung gesetzlicher Vorschriften und seiner berechtigten Geschäftsinteressen erheben und verarbeiten darf: Anrede, Nachname, Vorname, Geburtsdatum, Straße, Postleitzahl, Stadt und Land. Die folgenden Informationen dürfen auch über Mitarbeiter, Erfüllungsgehilfen und Unterauftragnehmer des Auftragnehmers erhoben werden, die eine Arbeits- oder Aufenthaltserlaubnis gemäß geltendem deutschem und europäischem Recht benötigen, um in Deutschland zu arbeiten: Gültigkeitsdauer der Arbeitserlaubnis und/oder Aufenthaltserlaubnis, Beschränkung der wöchentlichen Arbeitsstunden gemäß der Arbeitserlaubnis, Beschränkung des Einsatzortes gemäß der Arbeitserlaubnis, Beschränkung der Aufgaben/Position gemäß der Arbeitserlaubnis.

(7) Der Auftragnehmer darf Arbeitsergebnisse aus dieser Vereinbarung und alle Informationen über solche Ergebnisse nur nach vorheriger schriftlicher Zustimmung des Auftraggebers an Dritte weitergeben oder veröffentlichen.

(8) Jede Erwähnung des Auftraggebers als Referenz bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Auftraggebers. Einmal erteilt, bleibt diese Zustimmung gültig, bis sie widerrufen wird. Der Auftraggeber ist berechtigt, diese Zustimmung jederzeit ohne Vorankündigung und ohne Angabe von Gründen zu widerrufen.

(9) Wenn personenbezogene Daten vom Auftraggeber an den Auftragnehmer übermittelt und vom Auftragnehmer im Rahmen seiner Tätigkeiten verarbeitet werden, verpflichtet sich der Auftragnehmer, auf Verlangen des Auftraggebers die vom Auftraggeber angegebene Vereinbarung über die Auftragsverarbeitung personenbezogener Daten (ADV) abzuschließen.

(10) Die oben genannten Verpflichtungen gelten auch nach Ablauf der Vereinbarung weiter.

15. Einsatzverbot

(1) Der Auftragnehmer wird ausdrücklich darauf hingewiesen, dass es pensionierten Beamten, die die Deutsche Telekom Gruppe durch eine Vorruhestandsregelung verlassen, strikt verboten ist, jegliche weitere Tätigkeit, direkt oder indirekt, für die Deutsche Telekom Gruppe auszuüben. Dies gilt grundsätzlich auch für ehemalige Mitarbeiter der Deutschen Telekom Gruppe für einen Zeitraum von 15 Monaten nach Beendigung ihres Arbeitsvertrags, wenn sie im Zusammenhang mit der Beendigung eine Abfindung erhalten haben. Sofern die Beschaffungseinheit des Auftraggebers nicht bereits im Einzelfall schriftlich einen Ausnahmegenehmigung im Voraus erteilt hat, besteht zusätzlich ein allgemeines Einsatzverbot für aktuelle Mitarbeiter der Deutschen Telekom Gruppe.

(2) Vor diesem Hintergrund verpflichtet sich der Auftragnehmer seinerseits sicherzustellen, dass bei der Erbringung seiner Dienstleistung für den Auftraggeber die in Absatz 1 genannten pensionierten Beamten oder Mitarbeiter im Sinne von Absatz 1, Satz 3 nicht als Mitarbeiter oder Leiharbeiter oder als beauftragte Arbeits- oder Dienstleister oder in sonstiger Weise eingesetzt werden und keine der in Absatz 1 genannten ehemaligen Mitarbeiter als beauftragte Arbeits- oder Dienstleister oder als Leiharbeiter an Einheiten der Deutschen Telekom Gruppe verliehen werden.

(3) Im Falle eines Verstoßes gegen die Bestimmungen dieses Abschnitts 15 ist der Auftraggeber berechtigt, das Vertragsverhältnis aus wichtigem Grund zu kündigen. Darüber hinaus behält sich der Auftraggeber ausdrücklich das Recht vor, in diesem Zusammenhang Schadensersatzansprüche geltend zu machen.

16. Kündigung

(1) Der Auftraggeber kann jede Bestellung mit einer Frist von 2 Wochen kündigen.

(2) Wenn der Auftraggeber die Bestellung kündigt und bestimmte Kalendertage (bereits in der Bestellung angegeben) oder Stunden innerhalb dieser Kalendertage angefordert wurden, während derer die Dienstleistungen erbracht werden sollen, werden nur die Kalendertage oder Stunden bezahlt, die in den Zeitraum bis zum Ablauf der 2-wöchigen Kündigungsfrist fallen und für die tatsächlich Dienstleistungen erbracht wurden.

(3) Wenn die Kalendertage oder die Stunden innerhalb dieser Kalendertage, während derer die Dienstleistungen erbracht werden sollen, noch nicht in der Bestellung angegeben wurden und stattdessen der Auftraggeber Dienstleistungen aus einem in der Bestellung angegebenen volumenbasierten Tages-/Stundenkontingent innerhalb eines in der Bestellung definierten Zeitraums angefordert hat, werden lediglich die Tage/Stunden bezahlt, die angefordert wurden und während derer Dienstleistungen bis zum Ablauf der 2-wöchigen Kündigungsfrist erbracht wurden. Der Auftragnehmer ist nicht berechtigt, weitere Tages-/Stundensätze zu verlangen und/oder zu zahlen, beispielsweise im Rahmen einer „anteiligen Regelung."

(4) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.
Das Recht zur fristlosen Kündigung ist insbesondere zulässig, wenn eine Projektvereinbarung mit dem Kunden des Auftraggebers, für den die Dienstleistungen erforderlich sind, vorzeitig beendet wird.
Der Auftraggeber ist auch berechtigt, den Vertrag aus wichtigem Grund zu kündigen, wenn der Auftragnehmer (und/oder seine Unterauftragnehmer) die Anforderungen der geltenden Mindestlohngesetzgebung nicht erfüllen.
Darüber hinaus kann jede Bestellung von der Bestellpartei jederzeit und soweit gesetzlich möglich ohne Vorankündigung gekündigt werden:

i) wenn der Auftragnehmer sein Geschäft oder den Teil seines Geschäfts, der sich auf die vertraglichen Dienstleistungen bezieht, einstellt;
ii) wenn ein Antrag auf Eröffnung eines Insolvenzverfahrens in Bezug auf den Auftragnehmer gestellt wird;
iii) wenn ein Verfahren eröffnet oder ein Beschluss zur Auflösung, Liquidation oder Abwicklung des Auftragnehmers gefasst wurde, sei es freiwillig oder anderweitig (außer zum Zwecke einer solventen Fusion oder Umstrukturierung); oder
iv) wenn etwas Analoges zu den vorgenannten Ereignissen in der anwendbaren Gerichtsbarkeit eintritt.

17. Abtretung von Forderungen

(1) Forderungen des Auftragnehmers gegen den Auftraggeber dürfen nur mit ausdrücklicher schriftlicher Zustimmung der betroffenen Vertragseinheit des Auftraggebers abgetreten werden.

(2) Der Auftraggeber ist berechtigt, die aus diesem Vertrag oder einer Bestellung resultierenden Rechte und Pflichten ganz oder teilweise an ein verbundenes Unternehmen gemäß § 1 (1) ohne Zustimmung des Auftragnehmers abzutreten. § 345a HGB findet ausdrücklich Anwendung.

18. Aufrechnung

(1) Der Auftragnehmer hat kein Zurückbehaltungsrecht in Bezug auf seine vertraglichen Verpflichtungen oder in Bezug auf Eigentum, Daten oder Rechte des Auftraggebers.

(2) Der Auftragnehmer darf nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen aufrechnen.

19. Schlussbestimmungen

(1) Erfüllungsort ist der vom Auftraggeber angegebene Bestimmungsort.

(2) Diese EB und alle Bestellungen oder sonstigen Vereinbarungen, die in Bezug darauf getroffen werden, sowie alle daraus resultierenden Ansprüche, Rechte und Pflichten unterliegen dem Recht der Bundesrepublik Deutschland unter Ausschluss des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf, aller Kollisionsnormen und aller Standards, die auf andere Gesetze verweisen.

(3) Gerichtsstand ist der Hauptgeschäftssitz des Auftraggebers. Der Auftraggeber ist auch berechtigt, das Gericht am Hauptgeschäftssitz des Auftragnehmers anzurufen.

(4) Weicht die englische oder amerikanische rechtliche Bedeutung der Bestimmungen des Vertrags von der deutschen rechtlichen Bedeutung der Bestimmungen des Vertrags ab, so gilt die deutsche rechtliche Bedeutung. Jede Bezugnahme auf „gesetzliche Rechte“ oder „gesetzliche Bestimmungen“ oder „das Gesetz“ oder ähnliche Formulierungen gilt als Bezugnahme auf das geltende Recht.

(5) Sollten einzelne Bestimmungen dieses Vertrags oder einer Bestellung unwirksam oder undurchführbar sein oder werden, so berührt dies nicht die Wirksamkeit und Durchführbarkeit der übrigen Bestimmungen. In einem solchen Fall verpflichten sich die Parteien, die unwirksame oder undurchführbare Bestimmung durch eine wirksame und durchführbare Bestimmung zu ersetzen, die dem wirtschaftlichen Zweck und der Absicht der unwirksamen oder undurchführbaren Bestimmung so nahe wie möglich kommt. Das Gleiche gilt im Falle einer unvorhergesehenen Lücke im Vertrag oder einer Bestellung.

Signatures

Number of pages (including this one): 10

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

BWI
IT für Deutschland

Anforderung an die Informationssicherheit

Anlage 6 zum Rahmenvertrag über den Bezug von Konzeptions- und Entwicklungsleistungen für die „Strategische Partnerschaft pCloudBw“

Der Auftragnehmer erkennt die hier festgelegten Anforderungen zur Informationssicherheit an:

1 Allgemeine Anforderungen an die Informationssicherheit

1.1 Anwendungsbereich

Diese Anforderungen sind anwendbar, wenn der Auftragnehmer zur Erbringung der vertraglich vereinbarten Leistungen auf Informationen der BWI zugreift, diese verarbeitet oder speichert. Ergänzend wird bei Nutzung eines von der BWI bereitgestellten Clients auf die Richtlinie Informationssicherheit im Umgang mit Arbeitsmitteln verwiesen.

Dies bedarf Maßnahmen zum Schutz der IT-Systeme, -Applikationen, -Netze und firmenvertraulichen Informationen vor ungewollter Offenlegung, unberechtigtem Zugriff, Manipulation, Schadsoftware, Hacking, Cyberangriffen und anderer Bedrohungen. Dazu ist es erforderlich, dass Geschäftspartner von BWI die nachfolgenden Regeln und Grundsätze einhalten und Schutzmaßnahmen weder außer Betrieb nehmen, umgehen oder in sonstiger Weise verändern.

Der Auftragnehmer verpflichtet sich zusätzlich zu den sonstigen vertraglichen Vereinbarungen, die hierin definierten Regeln und Grundsätze zu beachten sowie diese Unterlage seinen Mitarbeitern, die Zugang oder Zugriff auf IT-Systeme, -Applikationen und -Netze der BWI oder firmenvertrauliche Informationen erhalten, zur Kenntnis zu bringen, sie auf die Einhaltung zu verpflichten und die Einhaltung in geeigneter Weise zu überprüfen.

Der Auftragnehmer wird alle Mitarbeiter und Dritte (Unterauftragnehmer), die an der Erbringung der Leistungen beteiligt sind, in angemessener Weise anweisen, die Sicherheits- und Compliance-Anforderungen dieser Anlage zu beachten.

1.2 Geheimhaltungsvereinbarung

Wenn der Auftragnehmer Informationen der BWI oder Zugang zu ihnen erhält, wird er alle Informationen vertraulich behandeln und nur zur Erfüllung der vertraglichen Verpflichtungen (die Leistungen) mit der gebotenen Sorgfalt verwenden. Jede weitere Nutzung bedarf der vorherigen schriftlichen Zustimmung der BWI. Dies gilt nicht für Informationen, an denen der Auftragnehmer nachweisen kann, dass er zum Zeitpunkt des Erhalts der Informationen bereits einen Rechtsanspruch hatte oder die ihm bereits allgemein bekannt waren oder die ihm von einem Dritten rechtmäßig zugänglich gemacht werden würden, ohne dass eine Verpflichtung zur Geheimhaltung besteht.

1.3 Informationssicherheitsmanagementsystem

Zur Erbringung der Leistungen muss der Auftragnehmer ein angemessenes Informationssicherheitsmanagementsystem (ISMS) nach allgemein anerkannten Standards (z.B. ISO 27001) einführen und kontinuierlich verbessern. Dieses ISMS muss die Anforderungen (abhängig von den zu erbringenden Leistungen/zu liefernden Produkten) gemäß folgendem Kapitel 2 "Technische und organisatorische Maßnahmen (TOM)" erfüllen.

BWI und der Auftragnehmer benennen jeweils einen Ansprechpartner für das Thema Informationssicherheit und informieren diese kontinuierlich.

Der Auftragnehmer ist verpflichtet, BWI unverzüglich über jeden Sicherheitsvorfall zu informieren, der die Sicherheit der BWI-Informationen und/oder der Leistungserbringung beeinträchtigt.

1.4 Prüfungsrechte und unabhängiger Prüfungsbericht

Der Auftragnehmer räumt BWI das Recht zur Prüfung und Überwachung der Leistungserbringung ein. Der Auftragnehmer wird BWI entsprechende Informations- und Zugriffsrechte (einschließlich Zugang zu Informationssystemen) einräumen.

Umfassen die Leistungen das Hosting der BWI-Informationen auf zentralen Systemen (z.B. Software-as-a-Service, Infrastructure-as-a-Service, IT-Hosting), so ist der Auftragnehmer verpflichtet, einen unabhängigen Auditbericht über die Wirksamkeit der Kontrollen für die Leistungserbringung vorzulegen.

1.5 Sub-Dienstleister (Unterauftragnehmer)

Der Auftragnehmer wird nur mit vorheriger schriftlicher Zustimmung der BWI Informationen an Dritte, wie z.B. Subdienstleister, auslagern oder an diese weitergeben. Der Auftragnehmer garantiert, dass die Sub-Dienstleister vertraglich an Informationssicherheitsanforderungen gebunden sind, die mindestens den Anforderungen dieser Anlage entsprechen.

1.6 Datenschutz

Soweit die Erbringung von Leistungen den Zugriff auf Daten erfordert, die den Datenschutzbestimmungen unterliegen, hält der Auftragnehmer die geltenden Datenschutzgesetze ein.

Dazu gehört auch die Einholung der schriftlichen Zustimmung der BWI, bevor BWI Daten einem internationalen Datentransfer (d.h. der Zugänglichmachung in einem anderen Drittland als in den vertraglichen Verpflichtungen des Auftragnehmers vorgesehen) unterzogen werden, es sei denn, alle entsprechenden internationalen Transfers erfolgen innerhalb der Europäischen Union bzw. in Länder mit einem angemessenen Datenschutzniveau, wie es die Europäische Union als angemessen erachtet.

Der Auftragnehmer wird mit BWI zusätzliche Vereinbarungen (z.B. Auftragsverarbeitungsvereinbarung) abschließen und BWI ermöglichen, Vereinbarungen mit Dienstleistern des Auftragnehmers zu treffen, wenn dies nach für BWI anwendbarem Recht erforderlich ist.

1.7 Aufbewahrung von Aufzeichnungen

Der Auftragnehmer wird BWI-Informationen unwiederbringlich löschen, sobald diese nicht mehr zur Erbringung der Leistungen oder zur Erfüllung gesetzlicher oder behördlicher Auflagen benötigt werden.

2 Technische und organisatorische Maßnahmen (TOM)

Die folgenden Abschnitte beschreiben technische und organisatorische Maßnahmen, die der Auftragnehmer im Rahmen seines Informationssicherheitsmanagementsystems umsetzen muss.

Diese TOM basieren auf dem internationalen Standard ISO 27002:2013 "Code of practice for information security controls".

2.1 Informationssicherheitsrichtlinien

Der Auftragnehmer muss umfassende Richtlinien für die Informationssicherheit nach anerkannten Industriestandards definieren, veröffentlichen und den Mitarbeitern des Auftragnehmers und relevanten externen Parteien mitteilen und regelmäßig überprüfen.

Beispiele für Best Practise:

- ISO 27001
- US NIST 800-53
- ISO 27001 auf der Basis von IT-Grundschutz (200-Standards)

2.2 2Organisation der Informationssicherheit

2.2.1 Interne Organisation

Der Auftragnehmer muss Rollen und Verantwortlichkeiten für die Informationssicherheit definieren und fähiges Personal einsetzen.

Beispiele für Best Practise:

- Informationsgüter im Eigentum des Auftragnehmers (z. B. IT-Anwendungen, Server, IT-Ausrüstung, IT-Leistungen),
- Verantwortung für die Informationssicherheit in der Projektabwicklung,
- umfassende Pflichten für die Informationssicherheit aller Mitarbeiter sowie der Vorgesetzten oder der Geschäftsleitung,
- die Ernennung spezieller Mitarbeiter wie Informationssicherheitsbeauftragte oder Datenschutzbeauftragte.

2.2.2 Mobile Geräte und Telearbeit

Der Auftragnehmer muss eine Richtlinie und unterstützende Sicherheitsmaßnahmen zur Minimierung von Risiken durch die Nutzung von mobilen Geräten und Telearbeitsplätzen einführen.

Beispiele für bewährte Verfahren:

- Registrierung von Mobilgeräten

- Standardkonfigurationen
- zentralisierte Verwaltung mit Lösungen für das Management mobiler Geräte (MDM)
- Zugangskontrolle
- Fernlöschung bei Verlust oder Diebstahl
- Richtlinie für die geschäftliche Nutzung von Geräten in Privatbesitz, falls zutreffend

2.3 Sicherheit im Personalwesen

2.3.1 Vor der Beschäftigung

Der Auftragnehmer führt vor der Einstellung Hintergrundprüfungen in Übereinstimmung mit den einschlägigen Gesetzen, Vorschriften und ethischen Grundsätzen durch. Hintergrundprüfungen müssen mindestens die Überprüfung der Vollständigkeit und Genauigkeit des Lebenslaufs des Kandidaten umfassen, einschließlich der behaupteten akademischen und beruflichen Qualifikationen, die für die Position relevant sind.

- Beispiele für bewährte Verfahren:
  - Anfragen zu Ausbildung und Referenzen bei Bewerbungsgesprächen,
  - Identitätskontrollen,
  - Polizeiliches Führungszeugnis.

Die Verantwortlichkeiten von Mitarbeitern und Auftragnehmern sind in schriftlichen Verträgen zu dokumentieren.

2.3.2 Während der Beschäftigung

Das Management des Auftragnehmers muss sicherstellen, dass Mitarbeiter und Auftragnehmer ihre Verantwortung für die Informationssicherheit kennen und erfüllen.

Beispiele für Best Practise:

- Verpflichtung der Unternehmensleitung für die Informationssicherheit,
- Regelmäßige Sicherheitsschulungen,
- Durchführung von Aufklärungsprogrammen für häufige Bedrohungen wie Phishing, Umgang mit vertraulichen oder persönlichen Informationen,
- Disziplinarmaßnahmen im Falle von Sicherheitsverletzungen.

2.3.3 Beendigung und Wechsel des Arbeitsverhältnisses

Der Auftragnehmer muss sicherstellen, dass bei Vertragsbeendigung die Interessen des Unternehmens und der Kunden kontinuierlich geschützt werden.

Beispiele für Best Practise:

- Rückgabe von Firmeneigentum (wie Laptops, Smartphones, Tablets, die sich im Besitz von Mitarbeitern, dem Auftragnehmern, Geschäftspartnern befinden) bei Beendigung des Vertrags,
- Aufhebung der Zugangsrechte zu Software, Systemen und/oder Räumlichkeiten,
- Kontrolle und Durchsetzung der Vertraulichkeitsvereinbarung für 10 Jahre nach Vertragsbeendigung.

2.4 Verwaltung von Vermögenswerten

2.4.1 Verantwortung für die Vermögenswerte

Der Auftragnehmer stellt sicher, dass alle mit Informationen und Einrichtungen und Systemen zur Informationsverarbeitung verbundenen Vermögenswerte (Information Assets) inventarisiert werden und ein für die Informationssicherheit verantwortlicher Eigentümer zugewiesen wird.

Beispiele für Best Practise:

- Information Assets umfassen Geschäftsprozesse und Informationen, IT-Gegenstände wie Hardware, Software, Netzwerk sowie Standorte, Organisationsstruktur, Personal und Leistungen,
- Zentrales Register für Anwendungen, Server, Infrastruktursysteme, Internetauftritte, Cloud Services, PCs, Laptops, Mobiltelefone und Tablets,
- Zuweisung der Verantwortlichkeit pro Anlage (z.B. eine bestimmte Anwendung) oder pro Anlagenklasse (z.B. alle Linux-Server an einem Standort),
- Siehe auch Abschnitt "Organisation der Informationssicherheit - Interne Organisation" oben.

2.4.2 Akzeptierte Nutzung von Informationsressourcen

Der Auftragnehmer muss die Mitarbeiter über geeignete, akzeptierte Nutzungsrichtlinien informieren. Wenn die Mitarbeiter des Auftragnehmers die Informationssysteme der BWI nutzen, müssen diese die entsprechenden Richtlinien der BWI einhalten.

Beispiele für Best Practise:

- Umgang mit Unternehmens- und Kundeninformationen
- Handhabung von IT-Geräten
- Handhabung von Passwörtern
- Sichere gemeinsame Nutzung von Daten mit Geschäftspartnern
- Erkennung und Behandlung von betrügerischen E-Mails (Phishing)
- Meldung von Informationssicherheitsvorfällen
- Nutzung des Internets

2.4.3 Klassifizierung der Informationen

Der Auftragnehmer stellt sicher, dass die Informationen hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit, Privatsphäre unter Berücksichtigung der potenziellen Geschäftsauswirkungen wie finanzielle Verluste, Prozessverzögerungen, Reputationsprobleme, Sicherheits-/Gesundheits-/Umweltprobleme klassifiziert werden.

Beispiele für Best Practise:

- Handhabung von Verfahren zum Schutz von Informationen während ihres gesamten Lebenszyklus (Erstellung, Verarbeitung, Übertragung, Vernichtung usw.) durch Maßnahmen wie Verschlüsselung,
- Die Kennzeichnung von Informationen ebenso wie die sichere Löschung ist zu entwickeln und konsequent anzuwenden.

2.4.4 Handhabung von Speichermedien

Der Auftragnehmer muss Verfahren zur sicheren Handhabung von Speichermedien, einschließlich Wechselmedien, physischem Transport und Entsorgung unter Berücksichtigung der darauf gespeicherten Informationen, definieren und umsetzen.

Beispiele für Best Practise:

- Speichermedien müssen sicher gelöscht oder physisch zerstört werden, wenn sie nicht mehr verwendet werden.
- Laptop-Festplatten müssen verschlüsselt werden.
- Die Mitarbeiter sind anzuweisen, USB-Flash-Laufwerke, externe Festplatten oder SD-Karten zu verschlüsseln, wenn darauf Kundendaten gespeichert sind, die zuvor nicht offiziell veröffentlicht wurden.
- Bei der physischen Übergabe von Medien ist eine Produkthistorie zu führen und zu dokumentieren.
- Wenn Medien nicht verschlüsselt werden können, dürfen sie nicht unbeaufsichtigt gelassen werden und müssen physisch übergeben werden (d.h. kein Versand per Post).

2.5 Zugriffskontrolle

Der Auftragnehmer verpflichtet sich, auf der Grundlage der Geschäfts- und Sicherheitsanforderungen zur Verhinderung von unberechtigten Zugriffen, angemessene Zugangskontrollkonzepte zu definieren, zu dokumentieren und umzusetzen, für die Fälle in denen

- BWI-Informationen, auf den Informationssystemen und/oder Speichermedien des Auftragnehmers gespeichert werden oder
- auf BWI-Informationssysteme durch das eigene Netzwerk des Auftragnehmers zugegriffen wird.

Solche Zugangskontrollkonzepte sollen

- die Zugangskontrollregeln und -rechte für jeden Benutzer oder jede Benutzergruppe eindeutig festlegen und
- sowohl den logischen Zugriff (z.B. Zugriff auf Programme und Daten) als auch den physischen Zugang (z.B. Zugang zu Gebäuden oder Datenverarbeitungsräumen) berücksichtigen und
- die Prozesse zur Verwaltung des Lebenszyklus des Benutzerzugriffs festzulegen.

Der Auftragnehmer muss über Technologie gemäß anerkannten Industriestandards verfügen, um die Zugangskontrollkonzepte angemessen umzusetzen.

Beispiele für Best Practise:

- Registrierung der Benutzer und ihrer Konten mit zentralisierten Identitäts- und Zugangsmanagement-Prozessen / -Systemen
- Workflows für Mitarbeiter, die in das Unternehmen eintreten oder es verlassen oder die Rolle im Rahmen ihres Arbeitsplatzes wechseln
- Vergabe von Zugriffsrechten nur bei Bedarf zur Erfüllung einer bestimmten Rolle im Rahmen ihres Arbeitsplatzes (Need-to-know-Prinzip)
- Workflows für die temporäre Vergabe von privilegierten (Administrator-) Zugriffsrechten, einschließlich der Überwachung der unter diesen Zugriffsrechten ausgeführten Aktivitäten
- Workflows für die Zuweisung, Erneuerung / Rücksetzung, Widerruf von Passwörtern und anderen Berechtigungen
- Workflows für die regelmäßige (mindestens jährliche) Überprüfung der Zugriffsrechte, die den IT-Benutzern zugewiesen wurden
- der Zugang zu IT-Systemen ist eingeschränkt und erfordert z.B. Benutzername/Passwort, elektronisches Zertifikat oder marktübliche biometrische Maßnahmen.

2.6 Kryptographie

Der Auftragnehmer muss sicherstellen, dass die Kryptographie ordnungsgemäß und effektiv zum Schutz der Informationen eingesetzt wird.

Beispiele für bewährte Verfahren:

- Verschlüsselung von Verschlusssachen während der Übertragung (z. B. E-Mail, Zugang zu Websites, Softwareschnittstellen),
- Verschlüsselung im Ruhezustand in Datenbanken oder Dateispeichern
- elektronische Signaturen wichtiger Dokumente
- Nutzung von gesicherten Web-Services für den Datenaustausch anstelle von unverschlüsselten E-Mails

- Nutzung und Schutz von kryptographischen Schlüsseln gemäß anerkannter Industriestandards und allgemein anerkannter Praktiken (Schlüsselverteilung, Speicherung, Wiederherstellung usw.).

2.7 Physikalische und umweltbezogene Sicherheit

Dieser Abschnitt ist anwendbar, wenn der Auftragnehmer Standorte betreibt, an denen BWI Informationen verarbeitet werden.

Der Auftragnehmer muss Schäden, Störungen und Interferenzen an Einrichtungen und Geräten und von Informationen innerhalb seiner Organisation durch organisatorische Maßnahmen, die Beschränkung des physischen Zugangs zu den Einrichtungen und den Schutz vor Umweltbedrohungen verhindern.

Beispiele für Best Practise:

- Einrichtungen zur Verarbeitung von Informationen sind durch eine physische Abgrenzung (wie Mauern und Zäune), Sicherheitswachen und Videoüberwachung an wichtigen Ein-/Ausgangspunkten geschützt, um unbefugten Zugang zu verhindern
- Wächter / Kartenleser / Smartcards zur Kontrolle und Aufzeichnung des Zugangs zu kritischen Bereichen wie Datenverarbeitungsanlagen
- Angemessene Auswahl der Standorte unter Berücksichtigung von Risiken wie Feuer, Überschwemmung, Erdbeben, Unruhen etc.
- Sicherheitsrichtlinien für Anlieferungs- und Verladebereiche
- Schutz der Energie- und Telekommunikationsverkabelung vor Abhören und Störungen, redundante Verkabelung zur Vermeidung von Ausfällen im Schadensfall
- Schutz der Ausrüstung in Ruhe und während des Transports, z.B. durch manuelle Zustellung statt Porto, unter Beachtung der Richtlinien für saubere Schreibtische

2.8 Betriebssicherheit

2.8.1 Betriebsprozesse und Verantwortlichkeiten, Backups, Installation von Software auf Betriebssystemen, Inhalte der Prüfung von Informationssystemen

Der Auftragnehmer muss den korrekten und sicheren Betrieb der Einrichtungen zur Verarbeitung von Informationen sicherstellen und gewährleisten, dass die Vorgänge innerhalb der betrieblichen Prozesse dokumentiert werden, einschließlich Änderungskontrollen, Beschränkung des Zugriffs auf Betriebssoftware, Backups & Wiederherstellung, Kapazitätsmanagement und Trennung der betrieblichen von anderen IT-Umgebungen.

Beispiele für Best Practise der Inhalte von Betriebsverfahren:

- Installation und Konfiguration von Systemen, einschließlich der Überprüfung der technischen Konformität der Systemkonfiguration

- Verarbeitung und Handhabung von Informationen, sowohl automatisiert als auch manuell, wie z.B. Schutz und Aufbewahrung von Ein- und Ausgabedateien, sichere Entsorgung der Ausgabe von fehlgeschlagenen Jobs
- Daten- und Infrastruktur-Backups
- Anforderungen an die Terminierung, einschließlich der Abhängigkeiten zu anderen Systemen, frühester Auftragsstart und späteste Auftragsabschlusszeiten
- Anweisungen für die Behandlung von Fehlern oder anderen unvorhergesehenen Situationen, die während der Auftragsausführung auftreten können, einschließlich Einschränkungen bei der Verwendung von System-Einrichtungen
- Support- und Eskalationskontakte einschließlich externer Supportkontakte im Falle unerwarteter betrieblicher oder technischer Schwierigkeiten
- systemspezifische Neustart- und Wiederherstellungsverfahren, die den allgemeinen Desaster-Recovery-Prozessen entsprechen
- Verwaltung von Audit-Trail- und Systemprotokollinformationen
- Kapazitätsmanagement
- Benutzer- und Zugriffsverwaltung, einschließlich der Segregation-of-Duties eine Definition der User-IDs des Systems
- Handhabung von Änderungen der Software-Lizenzanforderungen, die sich aus Installationen, De-Installationen, Konfigurationsänderungen oder Aktivitäten zur Benutzerverwaltung ergeben können
- Umgang mit Änderungen der Software- oder Infrastrukturkonfigurationen, Einstellungen oder Funktionalitäten
- technisches Schwachstellenmanagement

2.8.2 Schutz vor Schadsoftware

Der Auftragnehmer schützt Informationen und Einrichtungen zur Verarbeitung von Informationen mit branchenüblichen Maßnahmen vor Schadsoftware.

Beispiele für Best Practise:

- Einsatz von Schadsofware-Scannern auf PCs, Servern, Netzwerk-Gateways und mobilen Geräten
- regelmäßige Aktualisierung von Schadsoftware-Definitionen und Scan-Engines
- Sandbox-Technologie zur Erkennung noch unbekannter Schadsoftware

2.8.3 Protokollierung und Überwachung

Der Auftragnehmer protokolliert sicherheitsrelevante Ereignisse auf Informationssystemen wie Server, Netzwerk-Gateways, Mitarbeiterrechner, Schadsoftware-Scanner und anderer

Sicherheitstechnik. Die Protokolle sind gegen Manipulationen zu schützen und zu analysieren, um Sicherheitsvorfälle rechtzeitig zu erkennen.

Beispiele für Best Practise:

- Unbefugte Zugriffsversuche
- Änderungen an Benutzern, Gruppen, Zugriffsrechten, Geräte-Besitz, Sicherheitseinstellungen und Systemkonfiguration
- Nutzung von Privilegien
- Verwendung von System-Einrichtungen
- Start, Herunterfahren, An- oder Abmeldung des Informationssystems
- Zugriff (Versuche) auf Protokoll- und Programmdateien
- Zuordnung von IP-Adressen und Hostnamen
- Schreibzugriff auf Dateien und Objekte, wenn besondere Anforderungen an die Integrität bestehen
- Aktivierung und Deaktivierung von Schutzsystemen, wie z.B. Antiviren- und Intrusion Detection Systeme
- Warnungen von Sicherheitssystemen und Software
- Schutz von Log-Dateien vor unberechtigtem Zugriff (weder lesend noch schreibend)
- Es muss ausreichend Personal eingesetzt werden, um die Protokolle rechtzeitig zu überwachen und auf Sicherheitsvorfälle zu reagieren

2.8.4 Technisches Schwachstellenmanagement

Der Auftragnehmer muss technische Schwachstellen verwalten, einschließlich der Überwachung der Schwachstellen, der Risikobewertung, der Behebung (einschließlich Patches, Härtung, Einschränkungen von Softwareinstallationen oder anderer Maßnahmen, wenn keine geeigneten Patches verfügbar sind).

Beispiele für Best Practise:

- Einsatz von Schwachstellen-Scannern (z.B. Nessus)
- zu entscheiden, wie die erkannten Schwachstellen z.B. durch Patches von Anbietern und des Auftragnehmers behoben werden können
- Zeitpläne definieren, wann Schwachstellen auf der Grundlage der Kritikalität zu lösen sind
- die Installation von Software auf Client-Rechnern einzuschränken
- deaktivieren Sie nicht mehr benötigte Systemdienste

2.9 Kommunikation und Netzwerksicherheit

Dieser Abschnitt ist anwendbar, wenn der Auftragnehmer IT-Netzwerke zur Erbringung der Leistungen betreibt.

Der Auftragnehmer betreibt IT-Netzwerke zum Schutz von Informationen in Systemen und Anwendungen.

Beispiele für Best Practise:

- Segmentierung von Netzwerken, durch Firewalls getrennte Segmente
- Firewall-Regel-Lebenszyklus-Management vorhanden
- Intrusion Prevention System (IPS), im Falle des Outsourcings ist der Outsourcer verpflichtet, die anerkannte Sicherheitspraxis zu befolgen
- Sicherheitsereignisse werden protokolliert und die Protokolle werden zentral von einem SIEM-System analysiert

2.10 Systembeschaffung, -entwicklung und -wartung

Dieser Abschnitt ist anwendbar, wenn der Auftragnehmer IT-Systeme (Informationssysteme) zur Erbringung der Leistungen nutzt.

2.10.1 Sicherheitsanforderungen an Informationssysteme

Der Auftragnehmer stellt sicher, dass die Anforderungen an die Informationssicherheit bei der Beschaffung, Entwicklung und Wartung von Informationssystemen systematisch ermittelt und in den Entwicklungs- und Unterstützungsprozessen berücksichtigt werden.

Beispiele für Best Practise:

- Anforderungen an die Zugangskontrolle
- Einsatz von statischen Code-Analyse-Tools für selbstentwickelte Software
- Sicherheitspenetrationstests für Webanwendungen nach OWASP-Prinzipien
- Verschlüsselung von Informationen während der Übertragung und/oder bei der Speicherung (in Ruhe)
- digitale Signaturen
- spezifische Geschäftsprozessanforderungen wie z.B. Genehmigungen oder bestimmte Dokumentationen
- Vollständigkeitskontrollen

2.10.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen

Wenn der Auftragnehmer Informationssysteme entwickelt, muss er die Informationssicherheit innerhalb des Entwicklungslebenszyklus von Informationssystemen konzipieren und umsetzen. Dies umfasst Sicherheitsbewertungen, sichere Systementwicklungsverfahren, Änderungskontrollverfahren, angemessene Test- und Genehmigungsverfahren.

Beispiele für Best Practise:

- Regeln für die Entwicklung von Software und Systemen
- formale Änderungskontrollverfahren
- Überprüfung und Prüfung von Änderungen
- Grundsätze der sicheren Systemtechnik
- Umgebungen für Entwicklung / Test / Produktion
- Überwachung der ausgelagerten Systementwicklung
- Prüfung der Sicherheitsfunktionalität
- Abnahmetestprogramme, Schutz der Testdaten.

2.11 Einsatz von Unterauftragnehmern

Dieser Abschnitt ist anwendbar, wenn der Auftragnehmer zur Leistungserbringung Unterauftragnehmer einsetzt, die auf BWI-Informationen zugreifen, diese verarbeiten oder speichern können.

Der Auftragnehmer wird die schriftliche Zustimmung der BWI einholen, bevor ein Sub-Dienstleister erstmals Zugang zu BWI-Informationen erhält. Der Auftragnehmer stellt sicher, dass Regelungen in die Verträge mit Unterauftragnehmern aufgenommen werden, die Anforderungen dieser Anlage erfüllen. Der Auftragnehmer wird die Leistungserbringung seiner Subdienstleister regelmäßig überwachen, überprüfen und auditieren.

Beispiele für Best Practise:

- Zertifizierung für das Informationssicherheitsmanagement (z.B. ISO 27001)
- Anforderung von SOC2- oder ISAE 3000-Outsourcing-Berichten für Unterauftragnehmer (z.B. Cloud-Hosting-Anbieter)
- BWI erhält eine Kopie jedes für die Leistungen relevanten Unterauftrags für Auditzwecke (ohne Preisinformationen)
- Vereinbarung von Audit-Rechten mit Subunternehmern (z.B. ausgelagerter Rechenzentrumsbetrieb, ausgelagerte Softwareentwicklung)

2.12 Management von Informationssicherheitsvorfällen

Der Auftragnehmer muss Managementverantwortlichkeiten und -verfahren festlegen, um eine schnelle, effektive und ordnungsgemäße Reaktion auf Informationssicherheitsvorfälle zu

gewährleisten. Dies beinhaltet die Implementierung von Meldewegen und deren Nutzung durch Mitarbeiter und Dritte, die rechtzeitige Bewertung gemeldeter Ereignisse, die angemessene Reaktion auf Ereignisse, die als Sicherheitsvorfall gelten, angemessene Eskalations- und Kommunikationsverfahren, die Behebung von Problemen sowie Verfahren für forensische Beweise, die für disziplinarische oder rechtliche Maßnahmen erforderlich sind.

Beispiele für bewährte Verfahren:

- Sammlung von Informationssicherheitsereignissen von Servern, Netzwerk-Gateways, Endpunktgeräten und Sicherheitssystemen und deren Korrelation in einem SIEM-System;
- Sammeln von Sicherheitsereignissen vom IT-Servicedesk und von IT-Dienstleistern; Klassifizierungsskalen zur "Triage" und Bewertung von Informationssicherheitsereignissen hinsichtlich ihrer Kritikalität
- zentrale Teams zur Überwachung, Erkennung, Analyse und Berichterstattung von Informationssicherheitsereignissen und -vorfällen
- Integration von externen Quellen über Indikatoren für die Gefährdung (IOCs)
- Erstellung von Aufzeichnungen über Sicherheitsvorfälle sowohl auf technischer als auch auf Managementebene (z.B. in MISP- und Wiki-Systemen)
- Eskalation und Kommunikation an interne und externe Stakeholder oder Organisationen, einschließlich BWI

2.13 Aspekte der Informationssicherheit im Business Continuity Management

Der Auftragnehmer muss Prozesse, Verfahren und Kontrollen einführen, dokumentieren, implementieren und aufrechterhalten, um die Kontinuität der vertraglich vereinbarten Leistung zu gewährleisten.

Beispiele für Best Practise:

- Einrichtungen zur Verarbeitung von Informationen müssen mit einer ausreichenden Redundanz implementiert werden, um die Anforderungen an die Verfügbarkeit zu erfüllen
- Die Anforderungen an die Informationssicherheit müssen auch in Not-, Katastrophen- und Krisensituationen angemessen berücksichtigt werden

2.14 Compliance

2.14.1 Einhaltung der gesetzlichen und vertraglichen Anforderungen

Der Auftragnehmer stellt sicher, dass Verstöße gegen gesetzliche, behördliche, regulatorische oder vertragliche Verpflichtungen im Zusammenhang mit der Informationssicherheit und gegen jegliche Sicherheitsanforderungen vermieden werden.

Beispiele für Best Practise:

- Alle relevanten Anforderungen und die Vorgehensweise des Auftragnehmers zur Erfüllung dieser Anforderungen müssen für jedes Informationssystem und den Auftragnehmer explizit identifiziert, dokumentiert und auf dem neuesten Stand gehalten werden.
- Es sind geeignete Verfahren zu implementieren, um die Einhaltung der gesetzlichen, behördlichen und vertraglichen Anforderungen in Bezug auf die Rechte an geistigem Eigentum und die Nutzung proprietärer Softwareprodukte zu gewährleisten.
- Die Aufzeichnungen müssen vor Verlust, Zerstörung, Verfälschung, unbefugtem Zugriff und unbefugter Freigabe geschützt werden, in Übereinstimmung mit den gesetzlichen, behördlichen, vertraglichen und geschäftlichen Anforderungen.
- Die Privatsphäre und der Schutz personenbezogener Daten werden gemäß den einschlägigen Gesetzen und Vorschriften, soweit anwendbar, gewährleistet.
- Kryptographische Kontrollen werden in Übereinstimmung mit allen relevanten Vereinbarungen, Gesetzen und Vorschriften verwendet.

2.14.2 Überprüfung der Informationssicherheit

Der Auftragnehmer stellt sicher, dass die Informationssicherheit in Übereinstimmung mit den Richtlinien und Verfahren des Auftragnehmers implementiert und betrieben wird.

Beispiele für Best Practise:

- Der Ansatz des Auftragnehmers für das Management der Informationssicherheit und seine Umsetzung (d. h. Kontrollziele, Kontrollen, Richtlinien, Prozesse und Verfahren für die Informationssicherheit) sind in geplanten Abständen oder bei wesentlichen Änderungen unabhängig zu überprüfen.
- Die Manager müssen regelmäßig die Übereinstimmung der Informationsverarbeitung und der Verfahren in ihrem Verantwortungsbereich mit den entsprechenden Sicherheitsrichtlinien, -standards und sonstigen Sicherheitsanforderungen überprüfen.
- Die Informationssysteme sind regelmäßig auf die Einhaltung der Informationssicherheitsrichtlinien und -standards des Auftragnehmers zu überprüfen.

Signatures

Number of pages (including this one): 16

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

[redacted]

Aktenzeichen: xx

Vereinbarung zur Auftragsverarbeitung

Als Anlage zum Vertrag / zur Leistungsbeschreibung vom [*Datum*]

- nachfolgend „Leistungsvereinbarung“ -

zwischen

BWI GmbH, Auf dem Steinbüchel 22, 53340 Meckenheim

- nachfolgend „Verantwortlicher“ -

und

[*Vertragspartner*]

- nachfolgend „Auftragsverarbeiter“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhalt

Präambel....2
§ 1 Anwendungsbereich....2
§ 2 Konkretisierung des Auftragsinhalts....2
§ 3 Verpflichtungen und Weisungsbefugnis....2
§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter....4
§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle....4
§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter....5
§ 7 Löschung und Rückgabe von Daten....6
§ 8 Subunternehmen....6
§ 9 Datenschutzkontrolle....7
§ 10 Haftung und Schadenersatz....7
§ 11 Schlussbestimmungen....7
Anhang „Weisungsbefugnis“ zu § 3 (nach Zuschlagserteilung auszufüllen)....9
Anhang „Technisch-organisatorische Maßnahmen (TOM)“....10
Anhang „Subunternehmen“ zu § 8....12

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (*Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG* - DSGVO), und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich

(1) Die Vereinbarung findet Anwendung auf die Verarbeitung (Art. 4 Nr. 2 DSGVO) aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen und auf Weisung des Verantwortlichen verarbeitet werden. Nicht unter den Anwendungsbereich fallen Daten von Mitarbeitern des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

(2) Dieser Vertrag gilt vorranging vor anderen Vereinbarungen und Abreden zwischen Auftraggeber und Auftragnehmer, es sie denn, zwischen den Parteien wird ausdrücklich etwas anderes vereinbart.

§ 2 Konkretisierung des Auftragsinhalts

(1) Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten bestimmen sich nach der Leistungsvereinbarung, die dieser Vereinbarung angefügt ist.

(2) Folgende Arten personenbezogener Daten sind Gegenstand der Verarbeitung durch den Auftragsverarbeiter:

[Datenarten & -kategorien einfügen, bspw. Personenstammdaten, Kontaktdaten, bestimmte Gesundheitsdaten oder Verweis auf Leistungsbeschreibung im Anhang]

[Es ist durch den Auftragsverarbeiter zu prüfen, ob durch die technische Anwendung oder durch andere Umstände weitere personenbezogene Daten verarbeitet werden. Diese sind dann in der zuvor ersichtlichen Aufzählung zu ergänzen)

(3) Der Kreis der durch den Umgang mit ihren Daten betroffenen Personen ist (Kategorien betroffener Personen):

[Aufzählung und Beschreibung der betroffenen Personenkreise, bspw. Beschäftigte, Bewerbende, Veranstaltungsteilnehmende oder Verweis auf Leistungsbeschreibung im Anhang]

(4) Im Rahmen der Auftragsverarbeitung werden

☐ keine besonderen Kategorien von Daten

☐ besondere Kategorien von Daten

verarbeitet.

(5) Die verarbeiteten personenbezogenen Daten haben einen

☐ normalen Schutzbedarf

☐ hohen Schutzbedarf.

§ 3 Verpflichtungen und Weisungsbefugnis

(1) Die Vertragsparteien sind verpflichtet, die ihnen durch die Datenschutzgesetze (insb. DSGVO) auferlegten Pflichten einzuhalten. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

(2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen gemäß Kapitel 3 der DSGVO unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter der Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art 32 bis 36 DSGVO genannten Pflichten sowie insbesondere bei behördlichen Vorgängen wie beispielsweise Kontrollen durch Aufsichtsbehörden.

(4) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich, spätestens aber innerhalb von 3 Werktagen nach Eingang der Betroffenenanfrage an den Verantwortlichen weiterleiten.

(5) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(6) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten des Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind in der Anlage festgelegt.

(7) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

(8) Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher (oder dokumentierter elektronischer) Zustimmung durch den Verantwortlichen erteilen, es sei denn er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe verpflichtet.

(9) Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben, es sei denn er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe verpflichtet. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt.

(10) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in

das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(11) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich auf dem Gebiet

☐ der Bundesrepublik Deutschland

☐ der Europäischen Union (EU)

☐ des Europäischen Wirtschaftsraumes (EWR)

statt. Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage schriftlicher (oder dokumentierter elektronischer) Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der DSGVO im Einklang stehen. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

(12) Dem Auftragsverarbeiter wird widerruflich das Recht eingeräumt, unter folgenden Voraussetzungen die Datenverarbeitung außerhalb der Geschäftsräume (bspw. durch Außendienstmitarbeitende oder im Homeoffice oder in Telearbeit tätige Mitarbeitende) erbringen zu lassen:

- Die Verarbeitung von Daten des Verantwortlichen außerhalb der Geschäftsräume des Auftragsverarbeiters darf nur in den von dem Auftragsverarbeiter bekannten und genehmigten Räumlichkeiten aus erbracht werden. Der Auftragsverarbeiter trägt die vollständige Verantwortung dafür, dass alle Anforderungen an die technischen und organisatorischen Maßnahmen gemäß der von dem Verantwortlichen geprüften und genehmigten technischen und organisatorischen Maßnahmen (TOM) für die Verarbeitung von personenbezogenen Daten des Verantwortlichen durch den Auftragsverarbeiter erfüllt sind, der Mitarbeitende ausreichend über seine Pflichten unterwiesen wurde und der Auftragsverarbeiter ein jederzeitiges Kontrollrecht zu den TOMs hat.

- Besteht Grund zu der Annahme, dass sich Mitarbeitende des Auftragsverarbeiters bei der Datenverarbeitung außerhalb der Geschäftsräume nicht datenschutzkonform verhalten oder die TOMS nicht vollständig erfüllen, ist dem Mitarbeitenden das Recht auf Verarbeitung von Daten des Verantwortlichen außerhalb der Geschäftsräume unverzüglich zu entziehen.

Der Widerruf bedarf keiner Begründung. Bei Ausübung des Widerrufsrechts ist die Arbeitsleistung wieder am Betriebssitz des Auftragsverarbeiters zu erbringen.

☐ Der Auftragsverarbeiter verarbeitet keine Daten außerhalb der Geschäftsräume.

☐ Der Auftragsverarbeiter verarbeitet Daten außerhalb der Geschäftsräume.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung.

(3) Sofern der Auftragsverarbeiter der gesetzlichen Pflicht zur Benennung einer bzw. eines Datenschutzbeauftragte/n unterliegt sind die Kontaktdaten der/des Datenschutzbeauftragten zum Zwecke der direkten Kontaktaufnahme durch den Verantwortlichen hier einzufügen:

(…)

Unterliegt der Auftragsverarbeiter nicht der Benennungspflicht, teilt er dem Verantwortlichen die Kontaktdaten eines Ansprechpartners für den Datenschutz mit.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht und die Verarbeitung für den Verantwortlichen betroffen ist.

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in dem Anhang „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang „Technisch-organisatorische Maßnahmen“ wird Gegenstand dieser Vereinbarung.

(2) Ergibt eine vom Verantwortlichen durchzuführende Prüfung einen Anpassungsbedarf hinsichtlich der vom Auftragsverarbeiter zu ergreifenden technisch-organisatorischen Maßnahmen, sind die Anpassungen im Einvernehmen zwischen beiden Parteien umzusetzen.

(3) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/ Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Ein beauftragter Prüfer ist zur Verschwiegenheit verpflichtet und darf kein Wettbewerber des Auftragsverarbeiters sein.

(5) Die Überprüfung kann auch auf der Grundlage vorgelegter aktueller Testate, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit erfolgen. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(6) Die Überprüfung kann auch durch eine Inspektion vor Ort erfolgen. Der Verantwortliche kann sich hierzu in Abstimmung mit dem Auftragsverarbeiter in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen. Der Verantwortliche wird hierzu den Auftragsverarbeiter rechtzeitig von der Absicht einer Inspektion in Kenntnis setzen.

(7) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

(8) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

§ 7 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche im Auftrag des Verantwortlichen verarbeitete personenbezogene Daten dem Verantwortlichen zurückzugeben oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu löschen bzw. zu vernichten. Dies umfasst insbesondere dem Auftragsverarbeiter überlassene Daten, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen. Eine weitere Speicherung ist nur zulässig, wenn hierzu eine Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats besteht. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.

(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 8 Subunternehmen

(1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmen) nur nach einem der nachfolgenden Verfahren einsetzen: [Zutreffendes bitte ankreuzen]

☐ Der Auftragsverarbeiter darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Verantwortlichen gemäß dieser Vereinbarung durchführt, ohne vorherige gesonderte schriftliche (oder dokumentierte elektronische) Genehmigung des Verantwortlichen an einen Subunternehmer untervergeben. Der Auftragsverarbeiter reicht den Antrag für die gesonderte Genehmigung mindestens vier Wochen vor der Beauftragung des betreffenden Subunternehmers zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Subunternehmer findet sich im Anhang „Subunternehmen“. Die Parteien halten den Anhang jeweils auf dem neuesten Stand.

☐ Der Auftragsverarbeiter erhält die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Subunternehmen, die im Anhang „Subunternehmer zu § 8“ aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens vier Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Subunternehmen und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des betreffenden Subunternehmens Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter zu gewährleisten, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

(3) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortlichen berechtigt, auf schriftliche (oder dokumentierte elektronische) Anforderung vom Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.

(4) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 9 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, der/dem Datenschutzbeauftragten des Verantwortlichen zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag Zugang zu den üblichen Geschäftszeiten zu gewähren. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiter anweisen, mit dem/ der Datenschutzbeauftragten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 10 Haftung und Schadenersatz

Auf Artikel 82 DSGVO wird bezüglich der Haftung und des Rechts auf Schadenersatz verwiesen.

§ 11 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

_____	_____
Datum, Ort	Datum, Ort
_____	_____
Unterschrift (Verantwortlicher)	Unterschrift (Auftragsverarbeiter)
_____	_____
Name, Vorname, Funktion	Name, Vorname, Funktion

Anhang „Weisungsbefugnis“ zu § 3

Gemäß § 3 der Vereinbarung zur Auftragsverarbeitung hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten des Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind nachfolgend festgelegt.

Weisungsberechtigte Personen auf Seiten des Verantwortlichen:

- *X (Weisungsbefugter)*
- *XX (Stelllvertreter)*
- …

Zum Empfang der Weisungen berechtigte Personen auf Seiten des Auftragsverarbeiters:

- *Y (für … Bereich)*
- *YY (für … Bereich)*
- *YYY (Stellvertreter)*
- …

Vorgesehene Informationswege, wenn Weisung nach Meinung des Auftragsverarbeiters gegen datenschutzrechtliche Vorschriften verstößt:
[Zutreffendes bitte ankreuzen]

☐ schriftliche und/oder
☐ elektronische und/oder
☐ mündliche Information

Weisungen (auch mündliche Weisungen) sind durch die Vertragsparteien zu dokumentieren. Änderungen bei den weisungsbefugten Personen, den zum Weisungsempfang berechtigten Personen und bei den vorgesehenen Informationswegen sind dem Vertragspartner entsprechend unverzüglich anzuzeigen.

Anhang „Technisch-organisatorische Maßnahmen (TOM)“

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen
Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters
Der Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen
(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

☐ Der Auftragsverarbeiter verarbeitet keine Daten außerhalb der Geschäftsräume.

☐ Der Auftragsverarbeiter verarbeitet Daten außerhalb der Geschäftsräume.

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten	xxx
2.	Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung	xxx
3.	Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	xxx
4.	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	xxx
5.	Maßnahmen zur Identifizierung und Autorisierung der Nutzer	xxx
6.	Maßnahmen zum Schutz der Daten während der Übermittlung	xxx

7.	Maßnahmen zum Schutz der Daten während der Speicherung	xxx
8.	Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden	xxx
9.	Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen	xxx
10.	Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration	xxx
11.	Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit	xxx
12.	Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten	xxx
13.	Maßnahmen zur Gewährleistung der Datenminimierung	xxx
14.	Maßnahmen zur Gewährleistung der Datenqualität	xxx
15.	Maßnahmen zur Gewährleistung einer begrenzten Speicherdauer	xxx
16.	Maßnahmen zur Gewährleistung der Rechenschaftspflicht	xxx
17.	Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung	xxx
18.	Ggf. Beschreibung der spezifischen technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss	xxx

(2) Es ist ein Verfahren zu etablieren, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht.

(3) Folgende Nachweise werden dieser Vereinbarung angefügt: [Zutreffendes bitte ankreuzen]

☐ Einhaltung von Verhaltensregeln nach Artikel 40 DSGVO
☐ Zertifizierung nach Artikel 42 DSGVO
☐ Prüfberichte, Testate etc. unabhängiger Prüfer, bspw. Wirtschaftsprüfer, Auditoren, Datenschutzbeauftragte etc.
☐ geeignete Zertifizierung durch einen Auditprozess

Anhang „Subunternehmen“ zu § 8

Nach § 8 Abs. 1 S. 2 der Vereinbarung sind die zur Erfüllung dieses Vertrages bereits hinzugezogenen Subunternehmen zu bezeichnen. Gem. § 8 Abs. 1 S. 3 der Vereinbarung erklärt sich der Verantwortliche mit deren Beauftragung einverstanden.

Subunternehmen (Name, Anschrift bzw. Sitz)	**Datum des Abschlusses der Vereinbarung zur Auftragsverarbeitung**	**(Teil-)Leistungsgegenstand im Rahmen der Auftragsverarbeitung**

Signatures

Number of pages (including this one): 14

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

[redacted]

Aktenzeichen: xx

Vereinbarung zur weiteren Auftragsverarbeitung

Als Anlage zum Vertrag / zur Leistungsbeschreibung vom [*Datum*]

- nachfolgend „Leistungsvereinbarung“ -

zwischen

BWI GmbH, Auf dem Steinbüchel 22, 53340 Meckenheim

- nachfolgend „Auftragsverarbeiter“ -

und

[*Vertragspartner*]

- nachfolgend „weiterer Auftragsverarbeiter“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ -

wird die folgende Vereinbarung zur weiteren Auftragsverarbeitung geschlossen.

Inhalt

PRÄAMBEL....3
§ 1 ANWENDUNGSBEREICH....3
§ 2 KONKRETISIERUNG DES AUFTRAGSINHALTS....3
§ 3 VERPFLICHTUNGEN UND WEISUNGSBEFUGNIS....3
§ 4 BEACHTUNG ZWINGENDER GESETZLICHER PFLICHTEN DURCH DEN WEITEREN AUFTRAGSVERARBEITER....5
§ 5 TECHNISCH-ORGANISATORISCHE MAßNAHMEN UND DEREN KONTROLLE....5
§ 6 MITTEILUNG BEI VERSTÖßEN DURCH DEN WEITEREN AUFTRAGSVERARBEITER....6
§ 7 LÖSCHUNG UND RÜCKGABE VON DATEN....6
§ 8 SUBUNTERNEHMEN....6
§ 9 DATENSCHUTZKONTROLLE....7
§ 10 HAFTUNG UND SCHADENERSATZ....7
§ 11 SCHLUSSBESTIMMUNGEN....8
ANHANG „WEISUNGSBEFUGNIS“ ZU § 3 (NACH ZUSCHLAGSERTEILUNG AUSZUFÜLLEN)....9
ANHANG „TECHNISCH-ORGANISATORISCHE MAßNAHMEN (TOM)“....10
ANHANG „SUBUNTERNEHMEN“ ZU § 8....12

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein (weiteres) Auftragsverarbeitungsverhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG - DSGVO), und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren, haben die Vertragsparteien die nachfolgende Vereinbarung geschlossen.

§ 1 Anwendungsbereich

(1) Die Vereinbarung findet Anwendung auf die Verarbeitung (Art. 4 Nr. 2 DSGVO) aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen und auf Weisung des Auftragsverarbeiter verarbeitet werden. Nicht unter den Anwendungsbereich fallen Daten von Mitarbeitern des weiteren Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem weiteren Auftragsverarbeiter betreffen.

(2) Dieser Vertrag gilt vorranging vor anderen Vereinbarungen und Abreden zwischen Auftraggeber und Auftragnehmer, es sie denn, zwischen den Parteien wird ausdrücklich etwas anderes vereinbart.

§ 2 Konkretisierung des Auftragsinhalts

(1) Gegenstand und Dauer der weiteren Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten bestimmen sich nach der Leistungsvereinbarung, die dieser Vereinbarung angefügt ist.

(2) Folgende Arten personenbezogener Daten sind Gegenstand der Verarbeitung durch den weiteren Auftragsverarbeiter:

[Datenarten & -kategorien einfügen, bspw. Personenstammdaten, Kontaktdaten, bestimmte Gesundheitsdaten oder Verweis auf Leistungsbeschreibung im Anhang]

(3) Der Kreis der durch den Umgang mit ihren Daten betroffenen Personen ist (Kategorien betroffener Personen):

[Aufzählung und Beschreibung der betroffenen Personenkreise, bspw. Beschäftigte, BewerberInnen, Veranstaltungsteilnehmende oder Verweis auf Leistungsbeschreibung im Anhang]

(4) Im Rahmen der weiteren Auftragsverarbeitung werden

☐ keine besonderen Kategorien von Daten

☐ besondere Kategorien von Daten

verarbeitet.

(5) Die verarbeiteten personenbezogenen Daten haben einen

☐ normalen Schutzbedarf

☐ hohen Schutzbedarf.

§ 3 Verpflichtungen und Weisungsbefugnis

(1) Die Vertragsparteien sind verpflichtet, die Ihnen durch die Datenschutzgesetze (insb. DSGVO) auferlegten Pflichten einzuhalten. Der Auftragsverarbeiter kann jederzeit die Herausgabe, Berichtigung,

Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

(2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der weitere Auftragsverarbeiter den Auftragsverarbeiter angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.

(3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den weiteren Auftragsverarbeiter wendet, wird der weitere Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftragsverarbeiter weiterleiten.
(4) Der weitere Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Auftragsverarbeiters verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der weitere Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der weitere Auftragsverarbeiter dem Auftragsverarbeiter diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des weiteren Auftragsverarbeiters mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung des Auftragsverarbeiters. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Auftragsverarbeiter danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(5) Der weitere Auftragsverarbeiter hat den Auftragsverarbeiter unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der weitere Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Auftragsverarbeiters bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten des Auftragsverarbeiters sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des weiteren Auftragsverarbeiters sowie die vorgesehenen Informationswege sind in der Anlage festgelegt.

(6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

(7) Auskünfte an Dritte oder die betroffene Person darf der weitere Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher (oder dokumentierter elektronischer) Zustimmung durch den Auftragsverarbeiter erteilen, es sei denn er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe verpflichtet.

(8) Der weitere Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben, es sei denn er ist nach dem Unionsrecht oder dem Recht eines Mitgliedstaats zur Herausgabe verpflichtet. Kopien und Duplikate werden ohne Wissen des Auftragsverarbeiters nicht erstellt.

(9) Der Auftragsverarbeiter führt das Verzeichnis von Verarbeitungstätigkeiten im Auftrag i.S.d. Art. 30 Abs. 2 DSGVO. Der weitere Auftragsverarbeiter stellt dem Auftragsverarbeiter auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der weitere Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Auftragsverarbeiters durchgeführten Tätigkeiten der Verarbeitung.

(10) Die Verarbeitung der Daten im Auftrag des Auftragsverarbeiters findet ausschließlich auf dem Gebiet

☐ der Bundesrepublik Deutschland

☐ der Europäischen Union (EU)

☐ des Europäischen Wirtschaftsraumes (EWR)

statt. Jede Übermittlung von Daten durch den weiteren Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage schriftlicher (oder dokumentierter elektronischer) Weisungen des Auftragsverarbeiters oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der weitere Auftragsverarbeiter unterliegt, und muss mit Kapitel V der DSGVO im Einklang stehen. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

(11) Der weitere Auftragsverarbeiter gewährleistet, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Auftragsverarbeiters verarbeiten. Eine Verarbeitung von Daten außerhalb der Betriebsräume des weiteren Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) bedarf der vorherigen ausdrücklichen schriftlichen (oder dokumentierten elektronischen) Zustimmung des Auftragsverarbeiters, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den weiteren Auftragsverarbeiter

(1) Der weitere Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Auftragsverarbeiter auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem weiteren Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Der weitere Auftragsverarbeiter stellt dem Auftragsverarbeiter hierzu bei Bedarf entsprechende Informationen zur Verfügung.

(3) Sofern der weitere Auftragsverarbeiter der gesetzlichen Pflicht zur Benennung einer bzw. eines Datenschutzbeauftragte/n unterliegt sind die Kontaktdaten der/des Datenschutzbeauftragten zum Zwecke der direkten Kontaktaufnahme durch den Verantwortlichen hier einzufügen:

(…)

Unterliegt der weitere Auftragsverarbeiter nicht der Benennungspflicht, teilt er dem Auftragsverarbeiter die Kontaktdaten eines Ansprechpartners für den Datenschutz mit.

(4) Der weitere Auftragsverarbeiter informiert den Auftragsverarbeiter unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem weiteren Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in dem Anhang „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang „Technisch-organisatorische Maßnahmen“ wird Gegenstand dieser Vereinbarung.

(2) Ergibt eine vom Auftragsverarbeiter durchzuführende Prüfung einen Anpassungsbedarf hinsichtlich der vom weiteren Auftragsverarbeiter zu ergreifenden technisch-organisatorischen Maßnahmen, sind die Anpassungen im Einvernehmen zwischen beiden Parteien umzusetzen.

(3) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem weiteren Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das

Sicherheitsniveau der in dem Anhang „Technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Der weitere Auftragsverarbeiter wird dem Auftragsverarbeiter alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/ Inspektionen, die vom Auftragsverarbeiter oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen.

(5) Die Überprüfung kann auch auf der Grundlage vorgelegter aktueller Testate, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit erfolgen. Der weitere Auftragsverarbeiter verpflichtet sich, den Auftragsverarbeiter über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(6) Die Überprüfung kann auch durch eine Inspektion vor Ort erfolgen. Der Auftragsverarbeiter kann sich hierzu in Abstimmung mit dem weiteren Auftragsverarbeiter in den Betriebsstätten des weiteren Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

(7) Der weitere Auftragsverarbeiter stellt dem Auftragsverarbeiter darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

(8) Der weitere Auftragsverarbeiter hat im Benehmen mit dem Auftragsverarbeiter alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 6 Mitteilung bei Verstößen durch den weiteren Auftragsverarbeiter

Der weitere Auftragsverarbeiter unterrichtet den Auftragsverarbeiter umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der weitere Auftragsverarbeiter sichert zu, den Auftragsverarbeiter erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Auftragsverarbeiter oder den Verantwortlichen darf der weitere Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

§ 7 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftragsverarbeiters.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Auftragsverarbeiter, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der weitere Auftragsverarbeiter sämtliche im Auftrag des Auftragsverarbeiters verarbeitete personenbezogene Daten dem Auftragsverarbeiter zurückzugeben oder nach vorheriger Zustimmung des Auftragsverarbeiters datenschutzgerecht zu löschen bzw. zu vernichten. Dies umfasst insbesondere dem weiteren

Auftragsverarbeiter überlassene Daten, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen. Eine weitere Speicherung ist nur zulässig, wenn hierzu eine Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats besteht. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Auftragsverarbeiter auf Anforderung vorzulegen.

(3) Der weitere Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Auftragsverarbeiter übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 8 Subunternehmen

(1) Der weitere Auftragsverarbeiter darf noch weitere Auftragsverarbeiter (Subunternehmen) nur nach einem der nachfolgenden Verfahren einsetzen: [Zutreffendes bitte ankreuzen]

☐ Der weitere Auftragsverarbeiter darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Auftragsverarbeiter gemäß dieser Vereinbarung durchführt, ohne vorherige gesonderte schriftliche (oder dokumentierte elektronische) Genehmigung des Auftragsverarbeiter an einen Subunternehmer untervergeben. Der weitere Auftragsverarbeiter reicht den Antrag für die gesonderte Genehmigung mindestens vier Wochen vor der Beauftragung des betreffenden Subunternehmers zusammen mit den Informationen ein, die der Auftragsverarbeiter benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Auftragsverarbeiter genehmigten Subunternehmer findet sich im Anhang „Subunternehmen“. Die Parteien halten den Anhang jeweils auf dem neuesten Stand.

Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der weitere Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der weitere Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftragsverarbeiters auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wenn Subunternehmen durch den weiteren Auftragsverarbeiter eingeschaltet werden, hat der weitere Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Auftragsverarbeiter und dem weiteren Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

(3) Dem Auftragsverarbeiter sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Auftragsverarbeiter berechtigt, auf schriftliche (oder dokumentierte elektronische) Anforderung vom weiteren Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.

(4) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der weitere Auftragsverarbeiter gegenüber dem Auftragsverarbeiter für die Einhaltung der Pflichten des Subunternehmens. Der weitere Auftragsverarbeiter hat in diesem Falle auf Verlangen des Auftragsverarbeiters die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 9 Datenschutzkontrolle

Der weitere Auftragsverarbeiter verpflichtet sich, der/dem Datenschutzbeauftragten des Auftragsverarbeiters zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag Zugang zu den üblichen Geschäftszeiten zu gewähren. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiter anweisen, mit dem/ der Datenschutzbeauftragten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 10 Haftung und Schadenersatz

Auf Artikel 82 DSGVO wird bezüglich der Haftung und des Rechts auf Schadenersatz verwiesen.

§ 11 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des weiteren Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

_____	_____
Datum, Ort	Datum, Ort
_____	_____
Unterschrift (Auftragsverarbeiter)	Unterschrift (weiterer Auftragsverarbeiter)
_____	_____
Name, Vorname, Funktion	Name, Vorname, Funktion

Anhang „Weisungsbefugnis“ zu § 3 (nach Zuschlagserteilung auszufüllen)

zur Vereinbarung zur weiteren Auftragsverarbeitung vom [Datum]

zwischen BWI GmbH, Auf dem Steinbüchel 22, 53340 Meckenheim

und [Vertragspartner]

Der weitere Auftragsverarbeiter hat den Auftragsverarbeiter unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der weitere Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Auftragsverarbeiter bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten des Auftragsverarbeiters sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des weiteren Auftragsverarbeiters sowie die vorgesehenen Informationswege sind nachfolgend festgelegt.

Weisungsberechtigte Personen auf Seiten des Auftragsverarbeiters:

- X (Weisungsbefugter)
- XX (Stelllvertreter)
- …

Zum Empfang der Weisungen berechtigte Personen auf Seiten des weiteren Auftragsverarbeiters:

- Y (für … Bereich)
- YY (für … Bereich)
- YYY (Stellvertreter)
- …

Vorgesehene Informationswege, wenn Weisung nach Meinung des weiteren Auftragsverarbeiters gegen datenschutzrechtliche Vorschriften verstößt:
[Zutreffendes bitte ankreuzen]

☐ schriftliche und/oder
☐ elektronische und/oder
☐ mündliche Information

Weisungen (auch mündliche Weisungen) sind durch die Vertragsparteien zu dokumentieren. Änderungen bei den weisungsbefugten Personen, den zum Weisungsempfang berechtigten Personen und bei den vorgesehenen Informationswegen sind dem Vertragspartner entsprechend unverzüglich anzuzeigen.

Anhang „Technisch-organisatorische Maßnahmen (TOM)“

zur Vereinbarung zur weiteren Auftragsverarbeitung vom [*Datum*]

zwischen BWI GmbH, Auf dem Steinbüchel 22, 53340 Meckenheim

und [*Vertragspartner*]

§ 5 der Vereinbarung zur weiteren Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen
Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 Innerbehördliche oder innerbetriebliche Organisation des weiteren Auftragsverarbeiters
Der weitere Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen
(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten	xxx
2.	Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung	xxx
3.	Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	xxx
4.	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	xxx
5.	Maßnahmen zur Identifizierung und Autorisierung der Nutzer	xxx
6.	Maßnahmen zum Schutz der Daten während der Übermittlung	xxx

7.	Maßnahmen zum Schutz der Daten während der Speicherung	xxx
8.	Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden	xxx
9.	Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen	xxx
10.	Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration	xxx
11.	Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit	xxx
12.	Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten	xxx
13.	Maßnahmen zur Gewährleistung der Datenminimierung	xxx
14.	Maßnahmen zur Gewährleistung der Datenqualität	xxx
15.	Maßnahmen zur Gewährleistung einer begrenzten Speicherdauer	xxx
16.	Maßnahmen zur Gewährleistung der Rechenschaftspflicht	xxx
17.	Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung	xxx
18.	Ggf. Beschreibung der spezifischen technischen und organisatorischen Maßnahmen, die der weitere Auftragsverarbeiter zur Unterstützung des Auftragsverarbeiter ergreifen muss	xxx

(2) Es ist ein Verfahren zu etablieren, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht.

(3) Folgende Nachweise werden dieser Vereinbarung angefügt: [Zutreffendes bitte ankreuzen]

☐ Einhaltung von Verhaltensregeln nach Artikel 40 DSGVO
☐ Zertifizierung nach Artikel 42 DSGVO
☐ Prüfberichte, Testate etc. unabhängiger Prüfer, bspw. Wirtschaftsprüfer, Auditoren, Datenschutzbeauftragte etc.
☐ geeignete Zertifizierung durch einen Auditprozess

Anhang „Subunternehmen“ zu § 8

Nach § 8 Abs. 1 S. 2 der Vereinbarung sind die zur Erfüllung dieses Vertrages bereits hinzugezogenen Subunternehmen zu bezeichnen. Gem. § 8 Abs. 1 S. 3 der Vereinbarung erklärt sich der Auftragsverarbeiter mit deren Beauftragung einverstanden.

Subunternehmen (Name, Anschrift bzw. Sitz)	**Datum des Abschlusses der Vereinbarung zur weiteren Auftragsverarbeitung**	**(Teil-)Leistungsgegenstand im Rahmen der weiteren Auftragsverarbeitung**

Signatures

Number of pages (including this one): 13

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

Bundesministerium
für Wirtschaft
und Klimaschutz

Merkblatt für die Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD-Merkblatt)

Inhalt

Teil 1a): Über dieses Merkblatt - Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH: Rechte und Pflichten von öffentlichem VS-NfD-Auftraggeber und Unternehmen

Teil 1b): Vereinbarung über die Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH zwischen VS-NfD-Auftraggeber und VS-NfD-Auftragnehmer

Teil 2: Allgemeine Hinweise zum Umgang mit Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH

Teil 3: Anforderungen an Informationstechnik zur Verarbeitung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

Teil 4: Hinweise zur Kennzeichnung einer Verschlusssache des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH

Teil 5: Nachweis über die Verpflichtung

Teil 6: Vereinbarung über die Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH in der Privatwohnung (Homeoffice)

VS-NfD-Merkblatt
Teil 1a)

Über dieses Merkblatt - Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH: Rechte und Pflichten von öffentlichem VS-NfD-Auftraggeber und Unternehmen

1 VS-NfD-Auftrag

Vor der Weitergabe von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) an nichtöffentliche Stellen (Unternehmen[1]) muss mit diesen jeweils ein Vertrag geschlossen werden, in den die Bestimmungen dieses VS-NfD-Merkblatts (Anlage 4 zum Geheimschutzhandbuch - GHB) Eingang gefunden haben. Die konkreten geheimschutzrechtlichen Anforderungen eines VS-NfD-Auftrags sind zwischen VS-NfD-Auftraggeber und VS-NfD-Auftragnehmer zu klären. Dazu gehört auch die Einbeziehung von VS-NfD-Unterauftragnehmern (s. Ziff. 3.2)

2 VS-NfD-Auftraggeber und VS-NfD-Herausgeber

VS-NfD-Auftraggeber im Sinne dieses Merkblatts sind öffentliche Stellen oder Unternehmen, die Unternehmen (VS-NfD-Auftragnehmer) Zugang oder Zugangsmöglichkeit zu VS-NfD ermöglichen müssen[2]. Bei Unternehmen erfolgt dies in Form eines VS-NfD-Unterauftrags.
Die Bundesbehörden und bundesunmittelbaren öffentlich-rechtlichen Einrichtungen (Dienststellen), die eine VS-NfD erstellen oder deren Erstellung veranlassen, oder der Rechtsnachfolger dieser Dienststelle, sind VS-NfD-Herausgeber.

3 Rechte und Pflichten des VS-NfD-Auftraggebers

3.1 Öffentlicher VS-NfD-Auftraggeber

Bei Weitergabe von VS-NfD an Unternehmen muss der öffentliche VS-NfD-Auftraggeber mit dem Unternehmen einen Vertrag schließen, in den die Bestimmungen dieses Merkblatts Eingang gefunden haben (gemäß Ziff. 6.6 Abs. 2 Anlage V der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz - Verschlusssachenanweisung – VSA). Die hierin enthaltenen Kontrollrechte werden grundsätzlich vom öffentlichen VS-NfD-Auftraggeber ausgeübt. Weitergehende Maßnahmen, wie ein Geheimschutzverfahren des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) oder Sicherheitsüberprüfungen, sind für eine Weitergabe von VS-NfD nicht erforderlich.

3.2 Nicht-öffentlicher VS-NfD-Auftraggeber

Verschafft der VS-NfD-Auftragnehmer anderen Unternehmen (VS-NfD-(Unter-) Auftragnehmern) Zugang oder Zugangsmöglichkeit zu VS-NfD, hat er den VS-NfD-Unterauftragnehmer auf dieses Merkblatt zu verpflichten. Er nimmt in diesem Verhältnis die Rolle des VS-NfD-Auftraggebers ein und die entsprechenden Kontrollrechte werden dann von ihm ausgeübt.

[1] Der Begriff „nicht-öffentliche Stelle“ im Sicherheitsüberprüfungsgesetz (SÜG) umfasst vor allem Unternehmen der Wirtschaft und privatrechtlich verfasste Institutionen. Er wurde als gebräuchlicher Terminus aus dem BDSG übernommen. Im GHB und in diesem Merkblatt wird im Folgenden der Begriff „Unternehmen“ verwendet.
[2] Ein „VS-Auftrag“ liegt erst ab VS des Geheimhaltungsgrades VS-VERTRAULICH vor.

4 Pflichten des VS-NfD-Auftragnehmers

4.1 Allgemein

Der VS-NfD-Auftragnehmer verpflichtet sich, die Vorgaben sämtlicher Teile dieses Merkblatts einzuhalten. Auf mögliche strafrechtliche und vertragliche Konsequenzen bei Zuwiderhandlung wird ausdrücklich hingewiesen.

4.2 Nachweisliche Belehrung und Verpflichtung

Bevor eine Person Zugang oder Zugangsmöglichkeit zu VS-NfD erhält, ist sie vom Unternehmen über Teil 2 dieses Merkblattes zu belehren und auf dessen Einhaltung zu verpflichten. Dabei ist ihr ein Exemplar von den Teilen 2 und 4 dieses Merkblattes zugänglich zu machen. Wenn die Person Zugang oder Zugangsmöglichkeit zu VS-NfD auf Informationstechnik (IT) erhält, gilt gleiches zusätzlich für Teil 3 dieses Merkblattes. Die Belehrung, die Verpflichtung und der Empfang der erforderlichen Teile des Merkblatts sind durch Unterzeichnung des „Nachweises über die Verpflichtung“ (VS-NfD-Merkblatt Teil 5) durch die Person nachzuweisen. Der Nachweis muss vom VS-NfD-Auftragnehmer aufbewahrt werden und ist auf Nachfrage dem VS-NfD-Auftraggeber vorzulegen. Der Nachweis muss spätestens fünf Jahre nach dem Ausscheiden der betroffenen Person aus der Tätigkeit mit Bezug zu VS-NfD vernichtet werden.

4.3 Kontrollmöglichkeiten

Der VS-NfD-Auftraggeber berät den VS-NfD-Auftragnehmer über die Vorgaben dieses Merkblatts und kann sich über deren Einhaltung vergewissern.

4.4 Benennung einer für VS des Geheimhaltungsgrades VS-NfD verantwortlichen Person

Der VS-NfD-Auftragnehmer benennt eine für die Einhaltung und Durchführung der erforderlichen Maßnahmen zum Schutz von VS-NfD verantwortliche Person sowie ggf. eine/n Vertreter/in unter Nutzung des Teils 1b) dieses Merkblattes.
Der VS-NfD-Auftraggeber und der VS-NfD-Auftragnehmer erhalten jeweils eine Ausfertigung des unterschriebenen Teils 1b) des NfD-Merkblattes.

5 Übergangsfrist

Dieses Merkblatt (Teil 1a), Teil 1b), Teil 2, Teil 3, Teil 4, Teil 5, Teil 6) tritt zum 01.09.2023 in Kraft. Die Selbstakkreditierung gem. Teil 3 dieses Merkblattes ist bis zum 01.09.2025 durchzuführen.

VS-NfD-Merkblatt
Teil 1b)

Vereinbarung über die Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH zwischen VS-NfD-Auftraggeber und VS-NfD-Auftragnehmer

1. Der VS-NfD-Auftragnehmer verpflichtet sich, das VS-NfD-Merkblatt (Anlage 4 zum GHB) einzuhalten.

2. Der VS-NfD-Auftragnehmer benennt in Übereinstimmung mit datenschutzrechtlichen Vorschriften eine für die Einhaltung und Durchführung der erforderlichen Maßnahmen zum Schutz der Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) verantwortliche Person sowie ggf. ein/e Vertreter/in.

   Verantwortliche Person (geschäftliche Daten):

   ☐ Herr ☐ Frau Name, Vorname:

   Telefon-Nr. Mobilfunk-Nr.

   E-Mail-Adresse Anschrift

   Ggf. Vertreter/in der verantwortlichen Person (geschäftliche Daten):

   ☐ Herr ☐ Frau Name, Vorname:

   Telefon-Nr. Mobilfunk-Nr.

   E-Mail-Adresse Anschrift

3. Die Person ist im Auftrag des VS-NfD-Auftragnehmers dabei unter anderem für folgende Maßnahmen verantwortlich:

- Nachweisliche Belehrung und Verpflichtung der Mitarbeiter/innen des VS-NfD-Auftragnehmers, die Zugang oder Zugangsmöglichkeit zu VS-NfD erhalten, über bzw. auf VS-NfD-Merkblatt Teil 2, Teil 3 (sofern anwendbar) und Teil 4;
- Umsetzung der Vorgaben von Teil 3 dieses Merkblattes bei Verarbeitung von VS-NfD auf IT;
- Einholung der schriftlichen Einwilligung des VS-NfD-Auftraggebers zur Weitergabe von VS-NfD;
- Kontrolle der Einhaltung der erforderlichen Maßnahmen zum Schutz von VS-NfD im Unternehmen, ggf. auch bei VS-NfD-Unterauftragnehmern.

Ort, Datum

.....	.....
Unterschrift VS-NfD-Auftraggeber Dienststelle/Unternehmen:	Unterschrift VS-NfD-Auftragnehmer Unternehmen:

VS-NfD-Merkblatt
Teil 2

Allgemeine Hinweise zum Umgang mit Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH

1 Allgemeines

1.1 Anwendbarkeit

Die Regelungen dieses VS-NfD-Merkblattes gelten für deutsche VS-NfD sowie für ausländische vergleichbar eingestufte VS, die einem Unternehmen in Deutschland zur Aufbewahrung oder Verarbeitung überlassen worden sind. Gleiches gilt für bilaterale Geheimschutzabkommen, soweit dort nichts anderes geregelt ist.
Die Regelungen dieses VS-NfD-Merkblattes gelten nicht für VS über- oder zwischenstaatlicher Einrichtungen und Stellen (wie z. B. NATO, EU, ESA, OCCAR) mit vergleichbarem Geheimhaltungsgrad. Beim Schutz solcher VS sind die jeweiligen Vorschriften dieser Einrichtungen/Stellen zu beachten.

1.2 Kenntnis nur, wenn nötig

Von einer VS-NfD dürfen nur Personen Kenntnis erhalten, die auf Grund ihrer Aufgabenerfüllung Kenntnis haben müssen. Keine Person darf über eine VS-NfD umfassender oder eher unterrichtet werden, als dies aus Gründen der Aufgabenerfüllung notwendig ist. Es gilt der Grundsatz „Kenntnis nur, wenn nötig“.

1.3 Verstöße gegen die Geheimhaltungspflicht

Personen, die gegen die Vorschriften dieses VS-NfD-Merkblatts verstoßen, drohen Konsequenzen und eine strafrechtliche Ahndung des Verstoßes nach den §§ 93 bis 99, 203 Absatz 2 und 353b StGB.
Personen, die sich für den Umgang mit VS als ungeeignet erwiesen haben oder deren Geeignetheit nicht bewertet werden kann, werden von der für VS-NfD verantwortlichen Person von der Verarbeitung von VS-NfD ausgeschlossen.

1.4 Mitteilungspflichten bei Verlust von VS-NfD und Verstößen gegen Vorschriften dieses VS-NfD-Merkblatts

Der Verlust von VS-NfD sowie vermutete und festgestellte Verstöße gegen die Vorschriften dieses VS-NfD-Merkblatts sind unverzüglich der für VS-NfD verantwortlichen Person mitzuteilen. Diese informiert unverzüglich den VS-NfD-Auftraggeber. Mitteilungspflichten geheimschutzbetreuter Unternehmen nach GHB bleiben unberührt. Die erforderlichen Maßnahmen, um Schaden abzuwenden oder zu verringern und Wiederholungen zu vermeiden, werden unverzüglich getroffen. Die für VS-NfD verantwortliche Person bemüht sich um die Aufklärung des Sachverhalts.

1.5 VS-NfD auf IT

Bei Nutzung von IT beim Umgang mit VS-NfD ist zusätzlich Teil 3 dieses Merkblattes einzuhalten. Für die bearbeitenden Personen sind dort insbesondere die Vorgaben zur Verarbeitung in Ziff. 3 relevant.

2 Einstufung

Die Bundesbehörden und bundesunmittelbaren öffentlich-rechtlichen Einrichtungen (Dienststellen), die eine VS-NfD erstellen oder deren Erstellung veranlassen, oder der Rechtsnachfolger dieser Dienststelle, sind VS-NfD-Herausgeber.
Der VS-NfD-Herausgeber stuft eine VS in den Geheimhaltungsgrad VS-NfD ein, wenn deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann (§ 4 Absatz 2 Nummer 4 SÜG). Von einer Einstufung als VS-NfD ist nur Gebrauch zu machen, soweit dies notwendig ist.
Der VS-NfD-Herausgeber bestimmt, welche Informationen geheimhaltungsbedürftig sind. Das Unternehmen kann eine Einstufung nur auf Veranlassung des VS-NfD-Herausgebers vornehmen. Es ist stets nur deren Ersteller und nie selbst VS-NfD-Herausgeber. Das Unternehmen hat die erforderliche VS-NfD-Einstufung bei sich zu gewährleisten.

3 Befristung und Aufhebung der Einstufung

Die Einstufung einer VS-NfD ist auf 30 Jahre befristet. Der VS-NfD-Herausgeber kann, unter Berücksichtigung der Begründung für die Einstufung, eine kürzere Frist bestimmen. Die Einstufung endet mit Ablauf des Jahres, in welches das Fristende fällt. Die Frist kann nicht verlängert werden.
Entfällt die Geheimhaltungsbedürftigkeit einer VS-NfD, hat der VS-NfD-Herausgeber die Einstufung aufzuheben bzw. die Umsetzung durch das Unternehmen zu veranlassen. Die Aufhebung der Einstufung ist so zu vermerken, dass diese und die verfügende Stelle jederzeit erkennbar sind.

4 Kennzeichnung

Bei der Erstellung ist eine VS-NfD so zu kennzeichnen, dass bei ihrer Handhabung während der gesamten Dauer ihrer Einstufung jederzeit der Geheimhaltungsgrad, das erstellende Unternehmen, der VS-NfD-Herausgeber, das Datum der Einstufung sowie das vom Herausgeber festgelegte Ende der Einstufung (falls die Regelfrist von 30 Jahren unterschritten wird) erkennbar sind.
Die verbindliche Gestaltung der Kennzeichnung von VS-NfD ist dem Teil 4 dieses Merkblattes zu entnehmen.
Lässt die Beschaffenheit einer VS-NfD eine solche Kennzeichnung nicht zu, ist sinngemäß zu verfahren. Geheimhaltungsgrade sind grundsätzlich auszuschreiben soweit die Beschaffenheit einer VS dies zulässt. Ist dies nicht möglich, wird der Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH mit VS-NfD abgekürzt.
Im Falle nichtdeutscher VS eines entsprechenden Geheimhaltungsgrades sind diese zusätzlich mit dem deutschen Geheimhaltungsgrad zu kennzeichnen, sofern dies in den anwendbaren Geheimschutzabkommen vorgesehen ist.

5 Aufbewahrung

VS-NfD sind bei Nichtgebrauch in verschlossenen Behältern oder Räumen zum Schutz vor Kenntnisnahme durch Unbefugte (Grundsatz: „Kenntnis nur, wenn nötig“) aufzubewahren. Außerhalb von solchen Räumen oder Behältern sind sie auch dort so zu behandeln, dass eine Kenntnisnahme durch Unbefugte ausgeschlossen ist. Können VS-NfD nach der Aufgabendurchführung nicht vernichtet oder vollständig zurückgegeben werden, sind diese bis zur Aufhebung der Einstufung gemäß den Vorgaben dieses Merkblatts zu verwahren.
VS-NfD-Zwischenmaterial (z. B. Vorentwürfe) ist in derselben Weise zu schützen wie das Bezugsdokument.

6 Weitergabe

Weitergabe ist eine Übergabe oder Bereitstellung, durch die eine andere Person Zugang zu VS-NfD hat oder ihn sich verschaffen kann.

6.1 Erforderlichkeit

Vor jeder Weitergabe ist zu prüfen, ob diese unter Berücksichtigung des Grundsatzes „Kenntnis nur, wenn nötig“ zur Aufgabenerfüllung tatsächlich erforderlich ist.

6.2 Weitergabe innerhalb eines Unternehmens

VS-NfD können innerhalb eines Unternehmens offen weitergegeben werden, wobei auch hier gilt, dass eine Kenntnisnahme von Unbefugten ausgeschlossen sein muss. Eine Quittierung der Weitergabe ist nicht vorgesehen.

6.3 Weitergabe an Dritte (öffentliche Stellen oder Unternehmen)

Durch eine Weitergabe an einen Dritten hat dieser Zugang zur VS-NfD oder kann ihn sich verschaffen. Eine Weitergabe kann auch erforderlich sein, wenn ein Dritter sich gelegentlich einer Tätigkeit (z. B. Wartung, Reparatur), die für die Aufgabenerfüllung erforderlich ist, Zugang verschaffen kann. In diesem Fall sind Maßnahmen zu ergreifen, die einen Zugang zu der Verschlusssache verhindern (z. B. Technische Maßnahmen, Abdecken, Begleiten). Die Weitergabe von VS-NfD an Dritte ist nur zulässig, wenn vor der Weitergabe die Einwilligung des VS-NfD-Herausgebers nachweislich vorliegt. Der VS-NfD-Herausgeber kann im Einzelfall einwilligen, aber auch vorab bestimmten oder sämtlichen Weitergaben von VS-NfD im Rahmen eines oder mehrerer VS-NfD-Aufträge und VS-NfD-Unteraufträge innerhalb eines bestimmten Programms einwilligen. Die Einwilligung kann auch für Tätigkeiten erfolgen, bei denen sich ein Dritter gelegentlich der Ausführung eines Auftrages Zugang zu VS-NfD verschaffen kann. Diese Einwilligung ist über den VS-NfD-Auftraggeber einzuholen. Unternehmen dürfen sich auf eine schriftliche Erklärung des jeweiligen VS-NfD-Auftraggebers, dass eine solche Einwilligung des VS-NfD-Herausgebers vorliegt, verlassen. Sie bewahren die Erklärung als Nachweis auf.

6.4 Weitergabe an nichtdeutsche öffentliche Stellen und Unternehmen mit Sitz im Ausland

Auch eine Weitergabe an nichtdeutsche öffentliche Stellen (ausländische öffentliche Stellen oder über- oder zwischenstaatliche Einrichtungen und Stellen) und Unternehmen[1] mit Sitz im Ausland ist mit Zustimmung des VS-Herausgebers möglich. Dabei sind über die vorstehend angeführten Aspekte hinaus zusätzliche Anforderungen zu beachten:
Die Weitergabe von deutschen VS-NfD an nichtdeutsche öffentliche Stellen setzt grundsätzlich ein bilaterales Regierungs- oder Ressortgeheimschutzabkommen oder ein entsprechendes internationales Abkommen (Geheimschutzabkommen) voraus, welches die Bedingungen für die Weitergabe und weitere Handhabung regelt.
Die Weitergabe von VS-NfD an Unternehmen mit Sitz im Ausland erfolgt auf der Grundlage vertraglicher Vereinbarungen und grundsätzlich unter der Voraussetzung, dass in einem Geheimschutzabkommen mit dem Empfängerland der Schutz deutscher VS-NfD vereinbart worden ist.[2] Auf das Geheimschutzabkommen ist in der vertraglichen Vereinbarung zu verweisen.
Liegt kein bilaterales Regierungs- oder Ressortgeheimschutzabkommen oder ein entsprechendes internationales Abkommen vor, legt der VS-Herausgeber entsprechend der

[1] s. Teil 1a), Ziff. 1.
[2] Ob mit dem jeweiligen Empfängerland ein Geheimschutzabkommen besteht und ob darin eine Vergleichbarkeit mit VS-NfD vereinbart wurde, ist beim BMWK zu erfragen.

VSA im Einzelfall die Modalitäten der Weitergabe an nichtdeutsche öffentliche Stellen oder Unternehmen mit Sitz im Ausland im Benehmen mit BMWK fest.

6.5 Weitergabe durch private Zustelldienste

VS des Geheimhaltungsgrades VS-NfD können durch private Zustelldienste als gewöhnliche Brief- beziehungsweise Paketsendungen versandt werden. Der Umschlag beziehungsweise das Paket erhält keine VS-Kennzeichnung.

Auch grenzüberschreitend können VS-NfD durch private Zustelldienste wie oben beschrieben weitergegeben werden, es sei denn, das spezifische bilaterale Geheimschutzabkommen lässt die Weitergabe auf diesem Weg nicht zu oder der VS-NfD-Auftraggeber oder der VS-NfD-Herausgeber hat einer solchen Weitergabe widersprochen.

7 Mitnahme und mobiles Arbeiten

VS-NfD können außerhalb von Unternehmen nur auf Geschäftsreisen und zu Besprechungen mitgenommen werden, soweit dies zur Aufgabenerfüllung notwendig ist und sie angemessen gegen unbefugte Kenntnisnahme und unbefugten Zugriff gesichert werden. VS-NfD, u.a. Schriftstücke, können in diesem Fall in einem verschlossenen Umschlag unversiegelt mitgeführt werden.
Ihre Mitnahme zur Verarbeitung in der Privatwohnung ist grundsätzlich unzulässig. Die ausschließliche elektronische Verarbeitung von VS-NfD ist unter den Voraussetzungen von Teil 3, Ziff. 3.5 auch in der Privatwohnung zulässig. Der öffentliche VS-NfD-Auftraggeber kann weitere Ausnahmen zulassen. VS-NfD-Unterauftragnehmer dürfen sich auf eine schriftliche Erklärung ihres VS-NfD-Auftraggebers, dass eine solche Ausnahme zugelassen wurde, verlassen. Sie bewahren die Erklärung als Nachweis auf.
Zusätzlich zu der Ausnahmegenehmigung sind folgende Punkte einzuhalten:

- die Privatwohnung befindet sich innerhalb Deutschlands,
- die für VS-NfD verantwortliche Person erteilt die Zustimmung,
- der/die Mitarbeiter/in ist über spezifische Risiken des mobilen Arbeitens belehrt,
- Teil 6 dieses Merkblattes wurde von dem/der Mitarbeiter/in unterzeichnet und wird vom Unternehmen als Nachweis aufbewahrt.

8 Vernichtung

Um größere Bestände von VS-NfD zu vermeiden, sind nicht mehr benötigte VS-NfD zu vernichten oder an den VS-NfD-Auftraggeber zurückzugeben.
VS-NfD, auch VS-NfD-Zwischenmaterial, sind von den bearbeitenden Personen nur an den dafür vorgesehenen Orten so zu vernichten, dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann.
Für die Vernichtung dürfen grundsätzlich nur Produkte oder Verfahren eingesetzt oder Dienstleister beauftragt werden, die die Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erfüllen.

VS-NfD-Merkblatt
Teil 3

Anforderungen an Informationstechnik zur Verarbeitung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

1 Einleitung

1.1 Allgemeines

Wird Informationstechnik (IT) für die Verarbeitung von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) genutzt, sind neben den allgemeinen Schutzmaßnahmen der Teile 1 und 2 dieses Merkblattes zum Schutz der VS-NfD geeignete technische sowie organisatorische Maßnahmen zu treffen und deren Einhaltung regelmäßig zu kontrollieren. Zu den geeigneten technischen Maßnahmen zählen unter anderem IT-Sicherheitsprodukte, die über eine Zulassungsaussage (Zulassung oder Einsatzerlaubnis) des BSI verfügen und im vorgesehenen Einsatzkontext verwendet werden. Sofern nicht durch den VS-NfD-Auftraggeber oder das BSI andere Vorgaben existieren, sind die technischen und organisatorischen Maßnahmen zum Schutz der VS-NfD auf IT-Systemen in Ziff. 2 geregelt. Unabhängig von dem eingesetzten IT-System sind die Anforderungen an die Verarbeitung von VS-NfD gem. Ziff. 3 einzuhalten.

1.2 VS internationaler Organisationen (NATO, EU u.a.)

Bei der Verarbeitung von VS über- oder zwischenstaatlicher Einrichtungen und Stellen eines mit VS-NfD vergleichbaren Geheimhaltungsgrades gelten die jeweiligen Vorschriften dieser Einrichtungen/Stellen.

2 IT-System

Die technischen und organisatorischen Maßnahmen zum Schutz der VS-NfD auf IT-Systemen hängen von der Ausprägung des IT-Systems ab. Es gibt zwei Ausprägungen:

1. ein IT-System, das technisch isoliert („air-gapped“) betrieben wird (Ziff. 2.1) oder
2. ein IT-System, das mit anderen Netzwerken verbunden wird, die ein niedrigeres Sicherheitsniveau als VS-NfD haben (Ziff. 2.2).

Ein technisch isoliertes IT-System („air-gapped“) kann ein Einzelplatz-PC (Ziff. 2.1.1) oder ein Verbund eines IT-Systems (2.1.2) sein. Letzteres kann auch standortübergreifend vorliegen. Hierbei ist für die Übertragung ein IT-Sicherheitsprodukt mit Zulassungsaussage des BSI einzusetzen.

Die Verarbeitung von VS-NfD auf einem eigenen IT-System im Unternehmen ist unter Einhaltung folgender Voraussetzungen zulässig:

2.1 VS-NfD auf einem technisch isolierten IT-System („air-gapped“)

2.1.1 Einzelplatz-PC

Folgende technischen und organisatorischen Sicherheitsmaßnahmen sind umzusetzen:

- Zugangs-/Zugriffskontrolle:
  - Benutzung der Geräte erfolgt nur durch zugriffsberechtigte, auf das VS-NfD Merkblatt verpflichtete Personen,

  - Einrichtung von Benutzerprofil / restriktiven[1] Zugriffrechten sowie Login / Passwort um den Grundsatz „Kenntnis nur, wenn nötig“ umzusetzen.
- IT-Systeme, die nicht über eine Festplattenverschlüsselung mit Zulassungsaussage verfügen, sind vor Arbeitsende auszuschalten und im ausgeschalteten Zustand gemäß Teil 2, Ziff. 5 aufzubewahren;
- Es sind entsprechende Maßnahmen beim Patch- und Änderungsmanagement sowie zum Schutz vor Schadprogrammen zu treffen, wobei ein unbemerkter Abfluss von VS-NfD zu verhindern ist.
- Die Nutzung drahtloser Schnittstellen ist nicht gestattet;
- Deaktivierung nicht freigegebener drahtgebundener Schnittstelle;
- Einsatz einer geeigneten Festplattenverschlüsselung für mobile IT-Systeme und
- Einsatz eines IT-Sicherheitsproduktes mit Zulassungsaussage des BSI zum Ver-/Entschlüsseln von VS-NfD; Der bidirektionale Transfer mittels eines mobilen Datenträgers zwischen offenem Arbeitsplatz-PC und Einzelplatz-PC hat ausschließlich in verschlüsselter Form zu erfolgen. Es ist sicherzustellen, dass die Klartextdaten nicht auf dem mobilen Datenträger gespeichert werden, auch nicht temporär beispielsweise im Rahmen des Ver-/ Entschlüsselungsvorganges.

Eine Anwendung des IT-Grundschutzes des BSI ist hier nicht erforderlich.

2.1.2 Verbund eines IT-Systems

Neben den Sicherheitsmaßnahmen gemäß Ziff. 2.1.1 sind folgende Sicherheitsmaßnahmen zusätzlich umzusetzen:

- Mindestanforderung Datenablage: Daten unterschiedlicher VS-NfD-Aufträge müssen jeweils in separaten und ausschließlich für die jeweiligen zugriffsberechtigten Nutzer freigegebenen Projektordnern abgelegt werden; Seitens des Auftraggebers können weitergehende Anforderungen, bspw. ausschließliche Verwendung des IT-Systems für das jeweilige Projekt gefordert werden.
- Zentrale VS-NfD Komponenten: Zentrale VS-NfD Komponenten müssen nach dem Grundsatz „Kenntnis nur, wenn nötig“ im Serverraum physisch abgesichert werden. Dies kann durch eine Abtrennung in Form eines Käfigs oder einer vergleichbaren Abkastung (abschließbare Serverracks mit Einzelschließung etc.) erfolgen und
- Kommunikationsbeziehungen: Sämtliche Kommunikationsbeziehungen, insbesondere standortübergreifende, werden in einem Informationssicherheitskonzept (siehe Ziff. 4.2) beschrieben und hinsichtlich einer erforderlichen Verschlüsselung der VS-NfD durch ein IT-Sicherheitsprodukt mit Zulassungsaussage bewertet (hierzu Ziff. 3.4.1).

Ein auf das IT-System konzentriertes Informationssicherheitskonzept nach den gültigen Standards des IT-Grundschutzes des BSI ist hier nur dann erforderlich, wenn ein standortübergreifendes IT-Systems eingesetzt wird. In diesem Fall sind mindestens die Basisanforderungen umzusetzen (Ziff. 4.1). Der VS-NfD Auftraggeber kann darüber hinausgehende Anforderungen vorgeben.

[1] In einem gewöhnlich konfigurierten Betriebssystem erhält jeder Nutzer automatisch Vollzugriff auf alle Inhalte des Datenträgers mit Ausnahme der persönlichen Ordner anderer Nutzer. Seine Berechtigung für einzelne Ordner muss explizit ausgeschlossen werden (Opt-OUT). Der Grundsatz „Kenntnis nur, wenn nötig“ hingegen fordert eine explizite Zugriffserlaubnis für Nutzer, die nicht Ersteller sind (Opt-IN). Sonderregelungen bspw. für Projektgruppenordner, bei denen alle Nutzer automatisch Zugriff auf die gespeicherten Daten erhalten, sind im Informationssicherheitskonzept zu dokumentieren.

2.2 VS-NfD-Netzwerk verbunden mit Netzwerksegmenten, die nicht die VS-NfD Anforderungen erfüllen

Neben den Sicherheitsmaßnahmen gem. Ziff. 2.1.2 sind folgende Sicherheitsmaßnahmen für das VS-NfD-Netzwerk zusätzlich umzusetzen:

- Segmenttrennung: Physische oder zugelassene Trennung des VS-NfD-Netzwerksegments von anderen Netzwerksegmenten beispielsweise durch ein mehrstufiges Firewall System entsprechend der PAP-Struktur nach IT-Grundschutz des BSI.
- Firewall: Für die Firewall (PAP-Struktur) ist ein Regelwerk zu erstellen und regelmäßig anzupassen und zu überprüfen. Gegenstand dieses Regelwerkes sind insb. auch nach außen gerichtete Kommunikationsverbindungen. Die Initiierung des Zugriffs darf nur aus dem VS-NfD-Netzwerk erfolgen. Weiterhin müssen Softwareaktualisierungen, Telemetriefunktionen oder Entsprechende Konfigurationsempfehlungen, die den Abfluss von oder die Einsichtnahme in VS-NfD verhindern, sind umzusetzen und regelmäßig, insbesondere nach jedem Update, auf Veränderung zu überprüfen. Bei Auffälligkeiten sind unverzüglich weitere Schutzmaßnahmen vorzunehmen.
- Externe Schnittstellen: Sämtliche Schnittstellen sind bezogen auf die Kommunikation mit dem VS-NfD Netzsegment zu definieren und im Informationssicherheitskonzept zu beschreiben sowie in die Risikoanalyse aufzunehmen (siehe Ziff. 4.2).
- Schutz vor Schadprogrammen: Die Inhaltsprüfung auf Schadcode muss für Datenverkehr, der aus externen Netzwerken kommt, auf dem ALG (Application Layer Gateway) durchgeführt werden. Weiterhin muss allen IT-Systemen eine Software zur Erkennung von Schadcode eingesetzt werden. Diese darf keine Schadcodeprüfung außerhalb des VS-NfD Netzes, beispielsweise in der Cloud, durchführen.

Eine Anwendung des IT-Grundschutzes des BSI ist hier erforderlich. Es sind Basis- und Standardanforderungen (Ziff. 4.1) umzusetzen.

3 Anforderungen an die Verarbeitung von VS-NfD

Nachstehend werden die spezifischen Anforderungen zur elektronischen Verarbeitung von VS-NfD dargestellt. Die Verarbeitung beginnt bereits mit dem Lesen von VS-NfD auf IT.

3.1 Zulässige IT-Systeme und Freigabe

IT-Systeme zur Verarbeitung von VS-NfD müssen vor der ersten Nutzung durch die VS-NfD-verantwortliche Person freigegeben werden. Gleiches gilt für räumliche Arbeitsbereiche, die für die Verarbeitung von VS-NfD vorgesehen sind.
Private IT, Software oder Datenträger dürfen nicht für die Verarbeitung von VS eingesetzt werden.

3.2 Kennzeichnung von Datenträgern und Geräten

Datenträger, auf denen VS-NfD unverschlüsselt gespeichert werden, sind gemäß Teil 2, Ziff. 4 dieses Merkblattes zu kennzeichnen. Gleiches gilt für Geräte, in denen sich diese Datenträger befinden.

3.3 Wartung und Instandhaltung

Auf Datenträgern, die VS-NfD unverschlüsselt enthalten, sind die VS-NfD gemäß Ziff. 3.6 komplett zu löschen, bevor die Datenträger im Rahmen von Wartungs- oder Reparaturarbeiten am IT-System den persönlichen Gewahrsam der zugriffsberechtigten Personen verlassen.
Ist eine Löschung nicht möglich, sind die Datenträger auszubauen und zurückzuhalten. Ist das nicht möglich, gilt Teil 2, Ziff. 6.3 dieses Merkblattes.

3.4 Weitergabe über technische Kommunikationsverbindungen

3.4.1 Notwendigkeit der Verschlüsselung bei elektronischer Übertragung

VS-NfD müssen bei der elektronischen Übertragung grundsätzlich verschlüsselt werden mit Ausnahme Ziff. 3.4.2. Dazu sind ausschließlich IT-Sicherheitsprodukte[2] mit Zulassungsaussage einzusetzen.

3.4.2 Anforderungen zur unverschlüsselten Übertragung innerhalb von Liegenschaften

Wenn die Übertragung innerhalb einer Liegenschaft ausschließlich leitungsgebunden erfolgt und sämtliche Übertragungseinrichtungen, -leitungen, -verteiler und Trassen gegen unbefugten Zugriff geschützt sind, kann eine Verschlüsselung unterbleiben.

3.4.3 Telefonie / Fax

Telefonie und Fax-Übertragung sind nach Vornahme einer Risikobewertung Ende-zu-Ende verschlüsselt gestattet. Es gilt Ziff. 1.1.

3.4.4 Mobile IT-Systeme

Werden für die Verarbeitung oder Speicherung von VS-NfD tragbare IT-Systeme verwendet, so sind die Verschlusssachen durch IT-Sicherheitsprodukte mit Zulassungsaussage zu verschlüsseln. Von einer Verschlüsselung kann abgesehen werden, wenn die IT-Systeme innerhalb der Liegenschaft verbleiben, entweder im persönlichen Gewahrsam oder unter physischem Schutz (Teil 2, Ziff. 5).

3.4.5 Weitergabe in Notfallsituationen

Abweichend von Ziff. 3.4.1 ff. dürfen VS-NfD ausnahmsweise über nicht für VS-NfD zugelassene Kommunikationsverbindungen übermittelt werden, wenn die Übermittlung über eine BSI-zugelassene verschlüsselte Kommunikationsverbindung in einen vertretbaren Zeitrahmen nicht bereitgestellt werden kann. Die Details zu den abweichenden Rahmenbedingungen und Anforderungen werden für die jeweilige Notfallsituation vom VS-NfD-Auftraggeber gesondert festgelegt.
Wenn die Einbeziehung des VS-NfD-Auftraggebers zu einer Verzögerung führen würde, bei welcher der entstehende Schaden den mit einer Preisgabe der VS-NfD verbundenen Schaden deutlich überwiegen würde, kann die für VS-NfD verantwortliche Person ausnahmsweise die Festlegung selbst vornehmen. Der VS-NfD-Auftraggeber ist dann unverzüglich zu informieren. Mitteilungspflichten geheimschutzbetreuter Unternehmen nach GHB bleiben unberührt. In jedem Einzelfall ist die Einwilligung der für VS-NfD verantwortlichen Person einzuholen und zu dokumentieren.
In den Ausnahmefällen sind folgende Vorsichtsmaßnahmen zu beachten, damit das Risiko eines Informationsabflusses möglichst reduziert wird:

- Die Identität des Kommunikationspartners soll vor Beginn der Kommunikation festgestellt werden;

[2] Die Liste aktuell zugelassener IT-Sicherheitsprodukte und Systeme (BSI-Schrift 7164) befindet sich auf der BSI Homepage unter https://www.bsi.bund.de. Die jeweiligen Einsatz- und Betriebsbedingungen (E&B) stehen im geschützten Bereich des BMWK-Sicherheitsforums zum Download zur Verfügung. Nicht geheimschutzbetreute Unternehmen erhalten diese von ihrem VS-NfD-Auftraggeber. Die in den E&B beschriebenen Vorgaben sind zwingend umzusetzen. Eine abweichende Installation bzw. Konfiguration ist unzulässig. Wenn es keine IT-Sicherheitsprodukte mit Zulassungsaussagegibt, darf die Kommunikationsverbindung nicht verwendet werden.

- Die Kommunikation ist so zu führen, dass der Sachverhalt Dritten nicht verständlich wird und ein unmittelbarer Rückschluss auf den VS-NfD-Charakter nicht möglich ist;
- Die übermittelten VS-NfD dürfen keine Kennzeichnungen oder Hinweise aufweisen, die sie von einer nicht eingestuften Information unterscheiden. Die Kennzeichnungspflicht ist in diesem Fall aufgehoben und
- die Kommunikationspartner sind auf anderem Wege (zum Beispiel über andere technische Kommunikationsverbindungen, durch Post oder Kurier) unverzüglich über die Einstufung der VS-NfD zu unterrichten, außer, dies ist im Einzelfall nicht möglich oder nicht zweckmäßig. Der Kommunikationspartner muss die Kennzeichnung der VS-NfD, sofern möglich, nachholen.

3.5 Mitnahme und mobiles Arbeiten

Die ausschließlich elektronische Verarbeitung von VS-NfD ist auch in der Privatwohnung zulässig, wenn

- die genutzte IT (z. B. Notebooks) hierfür von der für VS-NfD verantwortlichen Person freigegeben (Ziff. 3.1) ist,
- sich die Privatwohnung innerhalb Deutschlands befindet,
- die für VS-NfD verantwortliche Person ihre Zustimmung erteilt hat,
- der/die Mitarbeiter/in über spezifische Risiken des mobilen Arbeitens belehrt ist und
- Teil 6 dieses Merkblattes von dem/der Mitarbeiter/in unterzeichnet wurde und vom Unternehmen als Nachweis aufbewahrt wird.

3.6 Löschen und Vernichten von Speichermedien die VS-NfD enthalten

Bevor Speichermedien den VS-NfD-Arbeitsbereich dauerhaft verlassen, müssen diese mittels BSI zugelassener bzw. freigegebener IT-Sicherheitsprodukte gelöscht werden. Ist eine Löschung nicht möglich, sind die Speichermedien nach den jeweils gültigen BSI-Vorgaben physisch zu vernichten.

3.7 IT-Administration

Die IT-Administration ist grundsätzlich durch eigenes Personal auszuführen. Es gilt Teil 2, Ziff. 6.3 dieses Merkblattes.

4 IT-Grundschutz des BSI

Je nach gewählter Ausprägung des IT-Systems ist der IT-Grundschutz des BSI in der jeweils geltenden Fassung in verschiedenem Umfang anzuwenden (Ziff. 1.1 f.).

4.1 Sicherheitsanforderungen

Der IT-Grundschutz des BSI in der jeweils geltenden Fassung basiert auf einer modularen Struktur, unterteilt in prozess- und systemorientierte Bausteine. In jedem Baustein werden die Sicherheitsanforderungen, die für den Schutz des betrachteten Gegenstands relevant sind, aufgeführt. Sie beschreiben, was zu dessen Schutz zu tun ist. Die Anforderungen sind in verschiedene Kategorien unterteilt, insbesondere in

- Basis-Anforderungen und
- Standard-Anforderungen, die auf den Basis-Anforderungen aufbauen.

Der notwendige Umfang der Umsetzung für die jeweilige Ausprägung des IT-Systems ergibt sich aus Ziff. 2. Die Anforderungen aus Ziff. 3 stellen einen zusätzlichen Baustein bei der Anwendung des IT-Grundschutzes dar.

4.2 Informationssicherheitskonzept und Risikoanalyse

Für das IT-System ist ein Informationssicherheitskonzept zu erstellen, welches die Anwendung des IT-Grundschutzes des BSI mit allen relevanten Sicherheitsanforderungen behandelt. Vom Unternehmen ist zu definieren, welche der Bausteine, in die der IT-Grundschutz des BSI unterteilt ist, für das IT-System zum Tragen kommen. Des Weiteren müssen die Auflagen nach VS-NfD-Merkblatt sowie eine Risikoanalyse mit einfließen. Bei Änderungen ist das Informationssicherheitskonzept inkl. der Risikoanalyse fortzuschreiben.

5 Selbstakkreditierung

Die für VS-NfD verantwortliche Person im Unternehmen bestätigt der Geschäftsleitung spätestens alle drei Jahre schriftlich die Umsetzung der Anforderungen aus Teil 3 (IT-Anforderungen) dieses Merkblattes (Selbstakkreditierung). Auf Anforderung ist dem VS-NfD-Auftraggeber bzw. dem BMWK diese Bestätigung auszuhändigen.

In der Selbstakkreditierung erklärt das Unternehmen,

1. die Umsetzung der IT-Anforderungen dieses Merkblatts in der jeweils gültigen Fassung,
2. sofern erforderlich, die Umsetzung der Einsatz- und Betriebsbedingungen der IT-Sicherheitsprodukte mit Zulassungsaussage und
3. die Etablierung eines ISMS durch:
    - die Anwendung der jeweils gültigen Standards des IT-Grundschutzes des BSI mit Erstellung eines Informationssicherheitskonzepts inkl. IT-Grundschutz-Check, Risikoanalyse und Umsetzungsplanung oder
    - eine ISO 27001 Zertifizierung auf Basis IT-Grundschutz oder
    - eine ISO 27001 Zertifizierung auf Basis einer anderen Grundlage mit Differenz-Analyse zum IT-Grundschutz (Zuordnungstabelle), wenn mindestens ein gleichwertiges Sicherheitsniveau zu den Anforderungen des IT-Grundschutzes gewährleistet ist.

Hinweise zur Kennzeichnung einer Verschlusssache des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH

1. Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) sind am oberen Rand mit dem voll ausgeschriebenen Geheimhaltungsgrad in schwarzer oder blauer Farbe zu kennzeichnen. Sollte eine VS-NfD aus mehreren Seiten bestehen, ist die Kennzeichnung am oberen Rand jeder beschriebenen Seite durchzuführen. Entsprechendes gilt auch für eingestufte Anlagen.
   Zusätzlich muss die Angabe enthalten sein, wer der Ersteller bzw. der VS-NfD-Herausgeber der VS-NfD ist, und wann die Erstellung bzw. Einstufung erfolgte.
   Lässt die Beschaffenheit einer VS-NfD die Kennzeichnung nicht zu, ist sinngemäß zu verfahren (z. B. Kennzeichnung in der zugehörigen Dokumentation).

2. Die Einstufungsfrist ist nur anzugeben, sofern diese die Regelfrist von 30 Jahren unterschreitet. In diesem Fall ist die Einstufungsfrist auf der ersten Seite der VS-NfD mit folgenden Vermerk anzugeben: „Die VS-Einstufung endet mit Ablauf des Jahres … .“
   Die Einstufung von VS-NfD ist spätestens nach 30 Jahren aufgehoben und kann nicht verlängert werden. Die Frist endet mit Ablauf des Jahres, in welches das Fristende fällt.

VS-NfD-Merkblatt
Teil 5

Nachweis über die Verpflichtung

Zutreffendes ist angekreuzt

Herr/Frau

Name, Vorname Geburtsdatum

wurde heute im Hinblick auf den beabsichtigten Zugang zu Verschlusssachen des Geheimhaltungsgrades

VS-NUR FÜR DEN DIENSTGEBRAUCH

über die Bestimmungen der §§ 93 bis 99, 203 Absatz 2 und 353b StGB unterrichtet, über die besonderen Bestimmungen des VS-NfD-Schutzes belehrt und auf deren gewissenhafte Erfüllung verpflichtet. Diese Verpflichtung gilt auch für die Zeit nach dem Ausscheiden aus dem Beschäftigungsverhältnis. Ihm/Ihr ist bekannt, dass ihm/ihr bei Verstößen gegen die oben genannten Bestimmungen vertrags- oder arbeitsrechtliche Maßnahmen und eine strafrechtliche Ahndung des Verstoßes nach den §§ 93 bis 99, 203 Absatz 2 und 353b StGB drohen können. Er/Sie hat eine Abschrift dieser Verpflichtung erhalten. Ihm/Ihr wurde ein Exemplar des VS-NfD-Merkblatts

☐ Teil 2 (Allgemeine Hinweise)
☐ Teil 3 (Hinweise zur Nutzung von IT)
☐ Teil 4 (Hinweise zur Kennzeichnung)
☐ Teil 6 (Behandlung von VS-NfD in der Privatwohnung)

ausgehändigt.

Ort, Datum

.....
Unterschrift des/der Verpflichteten

Vereinbarung über die Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH in der Privatwohnung („Homeoffice“)

1 Aufrechterhaltung des Schutzniveaus

Bei der Behandlung von VS-NfD in der Privatwohnung ist das durch das VS-NfD-Merkblatt vorgegebene Schutzniveau umzusetzen. Der/die Beschäftigte verpflichtet sich, die hierfür nötigen Maßnahmen in seiner/ihrer Privatwohnung zu treffen. Die Privatwohnung meint den in der Bundesrepublik Deutschland belegenen Wohnsitz des Beschäftigten.

2 Grundsatz „Kenntnis nur, wenn nötig“

Der Grundsatz „Kenntnis nur, wenn nötig“ ist einzuhalten. VS-NfD sind insbesondere vor der Einsicht durch andere, sich in der Privatwohnung befindliche Personen zu schützen. Dies ist durch geeignete organisatorische oder technische Maßnahmen sicherzustellen (z. B. Nutzung eines separaten Raumes, einfacher Verschluss bei Papieren und Material, Einhaltung von Teil 3 dieses Merkblattes bei IT-Verarbeitung), die den spezifischen Gefahren der Behandlung von VS in der Privatwohnung gerecht werden.

3 Nutzung von Informationstechnik (IT)

Für die Verarbeitung von VS-NfD auf IT ist Teil 3 des VS-NfD-Merkblattes zu einzuhalten. Insbesondere hält der/die Beschäftigte folgende Maßnahmen ein:

- Die IT-gestützte Verarbeitung von VS-NfD in der Privatwohnung darf nur auf von der für VS-NfD verantwortlichen Person freigegebenen IT-Systemen (Hardware und Software) erfolgen.
- IT-Systeme, die nicht über eine Festplattenverschlüsselung mit Zulassungsaussage verfügen, sind vor Arbeitsende auszuschalten und im ausgeschalteten Zustand gemäß Teil 2, Ziff. 5 aufzubewahren.
- Die eingesetzten IT-Systeme dürfen nicht mit IT-Geräten in der Privatwohnung oder außerhalb verbunden sein (Ausnahme: private Internetzugangsrouter, die für eine von der VS-NfD verantwortlichen Person freigegebene VS-NfD-Kommunikationsverbindung genutzt werden).
- Wartungs- oder Reparaturarbeiten an IT-Systemkomponenten dürfen nur auf Veranlassung der für den Schutz von VS-NfD im Unternehmen zuständigen Person durchgeführt werden.
- Die IT-Systeme dürfen nicht für private Zwecke verwendet werden.
- Einhaltung der von der VS-NfD verantwortlichen Person ausgehändigten Nutzungsanweisung für die IT-Systeme.

Der/die Beschäftigte ist über spezifische Risiken im „Homeoffice“ belehrt worden und bestätigt, diese Vorgaben des VS-NfD-Merkblatts und dieser Vereinbarung umzusetzen.

Ort, Datum

..... …….....

Unterschrift des/der Beschäftigten Unterschrift der für VS-NfD verantwortlichen Person

Signatures

Number of pages (including this one): 18

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

Bundesministerium
des Innern

Empfehlungen zur Korruptionsprävention in der Bundesverwaltung

Stand 9. Februar 2012

Empfehlungen zur Korruptionsprävention in der Bundesverwaltung

Inhaltsübersicht

Empfehlung zu Nr. 1 der Richtlinie:	Anwendungsbereich
Empfehlung zu Nr. 2 der Richtlinie:	Feststellen und Analysieren besonders korruptionsgefährdeter Arbeitsgebiete
Empfehlung zu Nr. 3 der Richtlinie	Mehr-Augen-Prinzip und Transparenz
Empfehlung zu Nr. 4 der Richtlinie:	Personal
Empfehlung zu Nr. 5 der Richtlinie:	Ansprechperson für Korruptionsprävention
Empfehlung zu Nr. 6 der Richtlinie:	Organisationseinheit zur Korruptionsprävention
Empfehlung zu Nr. 7 der Richtlinie	Sensibilisierung und Belehrung der Beschäftigten
Empfehlung zu Nr. 8 der Richtlinie:	Aus- und Fortbildung
Empfehlung zu Nr. 9 der Richtlinie:	Konsequente Dienst- und Fachaufsicht
Empfehlung zu Nr. 10 der Richtlinie:	Unterrichtungen und Maßnahmen bei Korruptionsverdacht
Empfehlung zu Nr. 11 der Richtlinie:	Leitsätze für die Vergabe
Empfehlung zu Nr. 12 der Richtlinie:	Antikorruptionsklausel, Verpflichtung von Auftragnehmern oder Auftragnehmerinnen nach dem Verpflichtungsgesetz
Empfehlung zu Nr. 14 der Richtlinie:	Zuwendungsempfänger
Empfehlung zu Nr. 15 der Richtlinie:	Besondere Maßnahmen

Anlagen

1. Aufzeichnungen über Beschaffungen
2. Niederschrift über die förmliche Verpflichtung
3. Sinngemäße Anwendung der Korruptionspräventionsrichtlinie (Musterklausel)
4. Verhaltensstandards zur Korruptionsprävention (Musterklausel und Anlage)

Empfehlungen zur Korruptionsprävention in der Bundesverwaltung

Die nachfolgenden Empfehlungen sind eine – nicht verbindliche - Umsetzungshilfe zur Richtlinie der Bundesregierung zur Korruptionsprävention in der Bundesverwaltung (Richtlinie).

Zu Nr. 1 der Richtlinie: Anwendungsbereich

Sinngemäß in Bezug auf Ziffer 1.2 bedeutet, dass die Richtlinie von den dort aufgeführten juristischen Personen des öffentlichen und des privaten Rechtes anzuwenden ist, soweit die abweichende Rechtsform dem nicht entgegen steht.

Zu Nr. 2 der Richtlinie: Feststellen und Analysieren besonders korruptionsgefährdeter Arbeitsgebiete

1. Verfahren zur Feststellung besonders korruptionsgefährdeter Arbeitsgebiete

1.1 Zur Feststellung der besonders korruptionsgefährdeten Arbeitsgebiete in einer Dienststelle werden alle Arbeitsgebiete auf ihre Korruptionsgefährdung untersucht. Vor Beginn der Feststellung sollen alle vorhandenen Informationen über die verschiedenen Arbeitsplätze/Dienstposten und Tätigkeiten (z. B. Organisationspläne, Geschäftsverteilungspläne) ausgewertet werden, um einen möglichst umfassenden Überblick über den Untersuchungsbereich zu erhalten. Die Erhebung der für die Feststellung darüber hinaus erforderlichen Informationen kann durch einen Fragebogen erfolgen. Die unten stehenden Merkmale für ein besonders korruptionsgefährdetes Arbeitsgebiet (s. u. Nr. 2) können entweder arbeitsplatz- bzw. dienstpostenbezogen oder aufgabenbezogen abgefragt werden. Nach Zusammenführung aller vorhandenen Daten trifft die untersuchende Organisationseinheit die abschließende Feststellung der besonderen Korruptionsgefährdung. Die Ergebnisse sollen für die gesamte Dienststelle zusammengestellt und dokumentiert werden (z.B. in einem Risikoatlas).

Eine ausführliche Hilfestellung zur Durchführung des Verfahrens enthält die Handreichung zur Feststellung besonders korruptionsgefährdeter Arbeitsgebiete vom 4. Januar 2012.

1.2 Die Feststellung kann in zwei Schritten erfolgen. In einem ersten Schritt werden die Arbeitsgebiete festgestellt, bei denen durch entscheidungserhebliches Verhalten von Beschäftigten Andere Vorteile von bedeutendem Wert erhalten (korruptionsgefährdete Arbeitsgebiete). Ausgehend von den korruptionsgefährdeten Arbeitsgebieten werden in einem zweiten Schritt die besonders korruptionsgefährdeten Arbeitsgebiete ermittelt.

2. Besonders korruptionsgefährdete Arbeitsgebiete

2.1 Besonders korruptionsgefährdet ist in der Regel ein Arbeitsgebiet,

a. bei dem durch entscheidungserhebliches Verhalten von Beschäftigten Andere bedeutende Vorteile erhalten können und

b. das mit mindestens einer der folgenden Tätigkeiten verbunden ist:
   - Tätigkeiten, die mit häufigen Außenkontakten verbunden sind, vor allem durch Kontroll- und Aufsichtstätigkeiten,
   - Bewirtschaften von Haushaltsmitteln im größeren Umfang, Vergabe von öffentlichen Aufträgen, Subventionen, Fördermitteln oder sonstigen Zuwendungen,
   - Erteilen von Auflagen, Konzessionen, Genehmigungen, Erlaubnissen und Ähnlichem, Festsetzen und Erheben von Gebühren,
   - Bearbeiten von Vorgängen mit behördeninternen Informationen, die für Andere nicht bestimmt sind.

Die obige Bestimmung der besonders korruptionsgefährdeten Arbeitsgebiete ist nicht abschließend. Auch bei Nichtvorliegen der Merkmale kann in besonders gelagerten Fällen eine besondere Korruptionsgefahr gegeben sein.

2.2 Die vorstehenden Kriterien sind in der Handreichung zur Feststellung besonders korruptionsgefährdeter Arbeitsgebiete erläutert.

3. Risikoanalyse

3.1 Bei besonders korruptionsgefährdeten Arbeitsgebieten soll
   - nach dem erstmaligen Feststellen der besonderen Korruptionsgefährdung,
   - nach organisatorischen oder verfahrensmäßigen Änderungen,
   - nach Änderungen der Aufgabeninhalte oder

- nach spätestens fünf Jahren

geprüft werden, ob eine Risikoanalyse durchzuführen ist. Hierzu werden für das jeweilige besonders korruptionsgefährdete Arbeitsgebiet die vorhandenen Sicherungen erfasst und deren Wirksamkeit kursorisch geprüft.

3.2 Wird nach der kursorischen Prüfung ein Handlungsbedarf erkannt, wird eine Risikoanalyse durchgeführt. Hierzu werden für das jeweilige Arbeitsgebiet die einzelnen Arbeitsabläufe und Prozesse sowie die bestehenden Sicherungen im Hinblick auf das Korruptionsrisiko untersucht. Anschließend wird bewertet, ob für die Risiken in dem notwendigen Maße wirksame Sicherungen bestehen. Wird ein Handlungsbedarf festgestellt, ist zu prüfen, wie die Aufbau-, Ablauforganisation und/oder die Personalzuordnung zu ändern sind. In diesem Fall enthält die Risikoanalyse Vorschläge und/oder die Anordnung zusätzlicher Maßnahmen.

Die für eine Risikoanalyse maßgeblichen Aspekte sind in Anlage 5 der Handreichung zur Feststellung besonders korruptionsgefährdeter Arbeitsgebiete aufgeführt.

Zu Nr. 3 der Richtlinie:
Mehr-Augen-Prinzip und Transparenz

1. Das Mehr-Augen-Prinzip als Maßnahme der Korruptionsprävention wird durch (Mit-) Prüfung und Kontrolle der Arbeitsergebnisse durch weitere Beschäftigte realisiert.

2. Das Mehr-Augen-Prinzip wird insbesondere durch Regelungen zur Mitzeichnung sichergestellt, die eine fachnahe Zweitprüfung vorsehen. Hierfür bieten sich in geeigneten Arbeitsbereichen IT-gestützte Arbeitsabläufe mit einhergehender Rollenverteilung (Workflows) an. Eine Mitzeichnung unter anderen fachlichen Aspekten oder lediglich unter Teilaspekten genügt dagegen den Anforderungen des Mehr-Augen-Prinzips nicht. Die entscheidungsbegründenden Unterlagen müssen für mitzeichnende Beschäftigte eine verständliche und hinreichende Informationsgrundlage für eine sachgerechte Prüfung bieten.

3. Sollte das Mehr-Augen-Prinzip ausnahmsweise nicht möglich sein, sollen geeignete und wirksame Ausgleichsmaßnahmen zur Korruptionsvorsorge (z. B. Verlagerung von Zuständigkeiten, besonders intensive Fach- und Dienstaufsicht) getroffen werden.

Zu Nr. 4 der Richtlinie:
Personal

1. Personalauswahl

Die für Personalangelegenheiten zuständige Organisationseinheit und die an einer Personalentscheidung beteiligten Vorgesetzten treffen bei der Besetzung von besonders korruptionsgefährdeten Dienstposten und Arbeitsplätzen eine Prognose zum Grad der Korruptionsgefährdung der betroffenen Personen. Die Prüfung ist in der Regel auf die Bewertung von bekannt gewordenen Auffälligkeiten beschränkt, z.B.

- straf- oder disziplinarrechtliche Ermittlungen,
- interne Ermittlungen wegen Korruptionsverdachts,
- Verschuldung, nicht geordnete wirtschaftliche Verhältnisse,
- soziale Probleme (z. B. Alkohol-, Drogen- oder Spielsucht),
- auffällige Verhaltensweisen, die die Zuverlässigkeit in Frage stellen.

Soweit solche Umstände bekannt werden, scheidet eine Verwendung der sich bewerbenden Person auf einem besonders korruptionsgefährdeten Dienstposten oder Arbeitsplatz solange aus, wie entsprechende Verfahren zur Überprüfung andauern bzw. der Verdacht nicht ausgeräumt ist.

2. Begrenzung der Verwendungsdauer

Die Umsetzung der Rotation erfordert, dass die Verwendungsdauer der Beschäftigten in besonders korruptionsgefährdeten Arbeitsgebieten erfasst wird. Die Verwendungsdauer beginnt mit der tatsächlichen Übertragung der besonders korruptionsgefährdeten Tätigkeit.

3. Umsetzung Rotation

3.1 Rotation kann sowohl durch den Wechsel der betroffenen Beschäftigten (Personalrotation) als auch durch den Wechsel der besonders korruptionsgefährdeten Aufgabe (Aufgabenrotation) auf einen bzw. zu einem anderen Arbeitsplatz/Dienstposten erfolgen. Die den Beschäftigten neu zu übertragenden Aufgaben können - aus anderen Gründen - wiederum besonders korruptionsgefährdet sein.

3.2 Sollte eine Rotation aus fachlichen oder (personal-)wirtschaftlichen Gründen (z. B. Mangel an Fachleuten) ausnahmsweise nicht möglich sein, sollen geeignete und wirksame Ausgleichsmaßnahmen zur Korruptionsvorsorge (z. B. Erweiterung des Mehr-Augen-Prinzips, Einführung von Teamarbeit, Verlagerung von Zuständigkeiten, besonders intensive Fach- und Dienstaufsicht) getroffen werden.

4. Die Ansprechperson für Korruptionsprävention ist kontinuierlich zu beteiligen.

Zu Nr. 5 der Richtlinie:
Ansprechperson für Korruptionsprävention

1. Die Ansprechperson für Korruptionsprävention soll förmlich bestellt werden. Ihre Bestellung soll in ihrem Zuständigkeitsbereich bekannt gemacht werden. Für die Ansprechperson soll eine Stellvertreterin oder ein Stellvertreter in gleicher Weise bestellt werden.

2. Die Ansprechperson soll in Verdachtsfällen in der Regel keine eigenen Ermittlungen anstellen.

3. Als Ansprechperson kommen auch anordnungsbefugte Beschäftigte in Betracht.

4. Zur Ansprechperson kann nicht bestellt werden, wer für Sicherheitsüberprüfungen nach Sicherheitsüberprüfungsgesetz (SÜG) zuständig ist.

5. Die Ansprechperson soll bei getrennter Aufgabenwahrnehmung mit den Beschäftigten der Inneren Revision und den für die Umsetzung der Richtlinie verantwortlichen Beschäftigten zusammenarbeiten.

6. Die Dienststelle unterstützt die Ansprechperson bei ihrer Aufgabenwahrnehmung (z. B. Einrichtung gesonderter elektronischer Postfächer, Bereitstellen geeigneter Räumlichkeiten).

7. Richtet sich der Verdacht gegen Dienststellenleitungen des nachgeordneten Geschäftsbereichs, informiert die angesprochene Ansprechperson die Ansprechperson der obersten Bundesbehörde. Dies kann auch in geeigneten anderen Fällen geschehen.

Zu Nr. 6 der Richtlinie:
Organisationseinheit zur Korruptionsprävention

Nach jeder Prüfung sollen die wesentlichen Prüfergebnisse in einer Schlussbesprechung mit den geprüften Organisationseinheiten erörtert werden.

Zu Nr. 7 der Richtlinie:
Sensibilisierung und Belehrung der Beschäftigten

1. Die aktive, vorausschauende Personalführung und –kontrolle kann auch der Sensibilisierung der Beschäftigten dienen.

2. Die regelmäßige Sensibilisierung der Beschäftigten kann insbesondere bei besonders korruptionsgefährdeten Arbeitsgebieten auch zum Bestandteil von Mitarbeitergesprächen werden.

Zu Nr. 8 der Richtlinie:
Aus- und Fortbildung

Aus- und Fortbildungsmaßnahmen im Bereich der Korruptionsprävention sollen insbesondere darauf ausgerichtet werden, der dort genannten Zielgruppe die erforderlichen Kenntnisse

- zur Wahrnehmung der Aufgaben nach den Nummern 2, 3, 5 bis 7 und 9 der Richtlinie und
- für das Herstellen eines Praxisbezugs im Dienstalltag

zu vermitteln.

Dabei soll die Schulung der Vorgesetzten diese fachlich in die Lage versetzen, ihrer Vorbild- und Kontrollfunktion gerecht zu werden. Beschäftigte in besonders korruptionsgefährdeten Arbeitsbereichen und deren Vorgesetzte sind zudem ebenengerecht mit den spezifischen Risiken der Korruption vertraut zu machen.

Hierzu erarbeiten die in den Ressorts zuständigen Stellen zeitliche, organisatorische und inhaltliche Vorgaben für eine systematische und ebenengerechte Schulung in den Aus- und Fortbildungseinrichtungen. Dabei sollen die Verantwortlichkeiten der beteiligten Dienststellen eindeutig festgelegt und abgegrenzt werden.

Zu Nr. 9 der Richtlinie:
Konsequente Dienst- und Fachaufsicht

1. Tritt in besonders korruptionsgefährdeten Arbeitsgebieten ausnahmsweise eine Verwendungsdauer von mehr als fünf Jahren auf (vgl. hierzu Empfehlung zu Nr. 4), soll die Dienst- und Fachaufsicht besonders intensiv ausgeübt werden. Hierzu gehört die regelmäßige Thematisierung korruptionsrelevanter Aspekte der Tätigkeit zwischen Vorgesetzten und Beschäftigten und die vermehrte stichprobenartige Überprüfung von Vorgängen unter dem Blickwinkel der Korruptionsprävention. Bei Behörden des Geschäftsbereichs soll auch eine Überprüfung vor Ort stattfinden. Zusammen mit der Ansprechperson für Korruptionsprävention sollen zusätzliche Ausgleichsmaßnahmen erörtert und umgesetzt werden.

2. Juristische Personen des öffentlichen und privaten Rechts, für welche die Richtlinie sinngemäß gilt, sollen in den Informationsaustausch der Ministerien mit ihrem jeweiligen nachgeordneten Bereich in geeigneter Weise und geeignetem Umfang einbezogen werden.

3. Im Falle einer Aufgabenübertragung auf eine nachgeordnete Behörde erstreckt sich die Dienst- und Fachaufsicht durch die vorgesetzte Dienstbehörde auch auf die konsequente Durchführung von Maßnahmen zur Korruptionsprävention. Hierbei sind die „Grundsätze zur Ausübung der Fachaufsicht der Bundesministerien über den Geschäftsbereich“ zu beachten.

Zu Nr. 10 der Richtlinie:
Unterrichtungen und Maßnahmen bei Korruptionsverdacht

Wenn es nachvollziehbare Anhaltspunkte oder Hinweise für eine Korruptionsstraftat gibt, sollte frühzeitig Kontakt mit der Staatsanwaltschaft aufgenommen werden, um zu klären, ob ein durch Tatsachen begründeter Verdacht besteht. Ggf. sollten in Abstimmung mit der Staatsanwaltschaft weitere behördeninterne Ermittlungen erfolgen. Der beteiligte Personenkreis ist dabei möglichst klein zu halten.

Zu Nr. 11 der Richtlinie:
Leitsätze für die Vergabe

1. Die Kontrolle der Vergabe öffentlicher Aufträge auf unzulässige Einflussfaktoren wird erheblich erleichtert, wenn – statt der vollständigen Vergabeakte – Aufzeichnungen geprüft werden können, die die wesentlichen Elemente einer Vergabe einschließlich des zeitlichen Ablaufs nach einem einheitlichen Schema wiedergeben. Daher sollten die Dienststellen - unabhängig von den Vorgaben des Vergaberechts - solche Aufzeichnungen führen (z.B. Muster - Anlage 1). Die Aufzeichnung kann auch in elektronischer Form generiert werden. Die Dienststellen entscheiden, ab welchen Auftragswerten sie solche Aufzeichnungen führen.

2. Die Dienststelle sorgt dafür, dass die Gründe, die ein Abweichen vom Vorrang der öffentlichen Ausschreibung beziehungsweise des offenen Verfahrens rechtfertigen, in jedem Einzelfall aktenkundig gemacht werden.

Zu Nr. 12 der Richtlinie:
Antikorruptionsklausel, Verpflichtung von Auftragnehmern oder Auftragnehmerinnen nach dem Verpflichtungsgesetz

1. Wird eine Antikorruptionsklausel verwendet, sollten potenzielle Bieter bereits in den Ausschreibungsunterlagen deutlich darauf hingewiesen werden, dass der Vertrag eine solche Klausel enthalten wird.

2. Eine Verpflichtung ist nur bei Personen erforderlich, die nicht bereits Amtsträger im Sinne des § 11 Abs. 1 Nr. 2 StGB sind. Beschäftigte von privatrechtlich organisierten Einrichtungen, die bei der Wahrnehmung von Verwaltungsaufgaben derart staatlicher Steuerung unterliegen, dass sie bei einer Gesamtbewertung der sie kennzeichnenden Merkmale gleichsam als „verlängerter Arm“ des Staates angesehen werden können, sind Amtsträger nach § 11 Abs. 1 Nr. 2 Buchstabe c StGB.

3. Im Übrigen bestimmt sich eine „Mitwirkung privater Unternehmen bei der Ausführung von Aufgaben der öffentlichen Hand“ nach § 1 Abs. 1 Nr. 1 und 2 des Verpflichtungsgesetzes. Ist unsicher, ob eine Person bereits Amtsträger ist oder verpflichtet werden kann, soll eine Verpflichtung (vorsorglich) erfolgen.

4. Verpflichtet werden sollen externe Personen, die aufgrund eines Auftrags für die Dienststelle tätig sind und für bestimmte Sachaufgaben, etwa als Gutachter oder Mitglied eines Beratungsgremiums, herangezogen werden (vgl. Anlage 2). Nicht zu verpflichten sind dagegen Beschäftigte externer Firmen, die bei einer Dienststelle handwerkliche Arbeiten verrichten, oder die Dienststelle mit Sachmitteln beliefern.

5. Welche (Dienst-) Stelle für die Verpflichtung zuständig ist, bestimmt sich nach § 1 Abs. 4 des Verpflichtungsgesetzes: Behörde im Sinne des § 1 Abs. 4 Nr. 1 des Verpflichtungsgesetzes ist die (Dienst-) Stelle, für die im Ergebnis die Leistung erbracht werden soll. Die Verpflichtung soll von der Organisationseinheit vorgenommen werden, die die externe Person beauftragt.

Zu Nr. 14 der Richtlinie:
Zuwendungsempfänger

1. Sofern Nr. 14.1 der Richtlinie im Rahmen institutioneller Förderungen die sinngemäße Anwendung der Richtlinie vorsieht, d. h. wenn durch Haushaltsrecht die Anwendung des Vergaberechts vorgesehen ist, soll die Musterklausel (Anlage 3) verwendet werden.

2. Wird im Rahmen institutioneller Förderungen durch Haushaltsrecht nicht die Anwendung des Vergaberechts aufgegeben, soll der Zuwendungsempfänger durch besondere Nebenbestimmungen im Zuwendungsbescheid bzw. durch Vereinbarung im Zuwendungsvertrag zur Einhaltung von Verhaltensstandards (Anlage 4) verpflichtet werden.

3. Im Rahmen des Zuwendungsverhältnisses soll der Zuwendungsgeber die tatsächliche Umsetzung dieser Vorgaben prüfen und sicherstellen. Die Zuwendungsempfänger sollen die konkrete Umsetzung im Sachbericht schildern.

Zu Nr. 15 der Richtlinie:

Bei juristischen Personen des Privatrechts, an denen der Bund mehrheitlich und unmittelbar beteiligt ist, sollen die beteiligungsführenden Stellen des Bundes im Rahmen der ihnen unter Berücksichtigung der Rechtsform und der Beteiligungsverhältnisse zustehenden Einflussmöglichkeiten auf

die sinngemäße Anwendung der Richtlinie zur Korruptionsprävention und, wenn dies nicht möglich ist, auf sonstige geeignete Maßnahmen zur Korruptionsprävention hinwirken.

Muster zu Nr. 11 der RL **Anlage 1**

Datenblatt Beschaffungen

1. Vorgangsdaten
Referat:
Auftragsnummer/Vorgangsnummer:
Aktenzeichen:
Bearbeiter/-in (Beschaffer/-in):
Auftragsgegenstand:
Schätzpreis:
Auftragswert:
Rechnungswert (brutto):

2. Bedarfsmeldung
Bedarfsträger:
Bedarfsmitteilung vom:
Bedarfsbegründung und -beschreibung geprüft am:
Zur Beschaffung freigegeben am:

3. Leistungsbeschreibung
Leistungsbeschreibung erstellt am:
Leistungsbeschreibung erstellt durch:
Hierbei ggf. bereits vorgegebener Hersteller:

4. Vergabeart:
Offenes Verfahren / Öffentliche Ausschreibung Nicht offenes Verfahren / Beschränkte Ausschreibung Verhandlungsverfahren / Freihändige Vergabe Abruf aus Rahmenvertrag
Entscheidung über Vergabeart begründet und dokumentiert am:

5. Auftragsvergabe
Angebote ausgewertet am/durch:
Zuschlag erteilt am/durch:
Auftrag erteilt am/durch:

6. Auftragnehmer
Name und Anschrift:
Vorgangsnummern anderer Aufträge an diesen Auftragnehmer:

7. Lieferung/Güteprüfung
Lieferschein vom:
Geliefert am:
Mängelfreiheit:
ja - Bestätigung am/durch:
nein - Reklamation am/durch:
Nacharbeit:
Reklamation erledigt am/bestätigt durch:
Inventarisierung erfolgt am:
Inventarnummer(n):

8. Zahlung
Nachweis rechnerische Richtigkeit am/durch:
Nachweis sachliche Richtigkeit am/durch:
Skonto (Betrag):
Zahlungsanordnung am/durch:
Zahlung erfolgt am:
Haushaltsstelle:
Zahlungsempfänger

Muster zu Nr. 12.2 der RL **Anlage 2**

Verpflichtung der Auftragnehmerseite nach dem Verpflichtungsgesetz

Niederschrift über die förmliche Verpflichtung von Auftragnehmern und Auftragnehmerinnen nach dem Verpflichtungsgesetz

Herr/Frau _____
Auftragnehmer/in _____
ist nach § 1 Abs. 1 des Verpflichtungsgesetzes von
Herrn/Frau _____
Auftraggeber/in _____

auf die gewissenhafte Erfüllung seiner / ihrer Obliegenheiten verpflichtet worden.
Auf die strafrechtlichen Folgen einer Pflichtverletzung wurde hingewiesen. Der / Die Verpflichtete wurde darüber informiert, dass er / sie durch die Verpflichtung bei der Anwendung der folgenden Vorschriften des Strafgesetzbuches Amtsträgern gleichgestellt wird:

Korruptionsstraftaten:

§§ 331, 332, 335, 336, 338, 358	Vorteilsannahme und Bestechlichkeit.

Geheimnisverrat/Vertraulichkeitsverletzung:

§§ 353 b, 358	Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht,
§§ 355, 358	Verletzung des Steuergeheimnisses,
§ 201 Abs. 3	Verletzung der Vertraulichkeit des Wortes,
§ 203 Abs. 2, 4, 5	Verletzung von Privatgeheimnissen,
§ 204	Verwertung fremder Geheimnisse,
§ 97 b Abs. 2 i. V. m. §§ 94 bis 97	Verrat in irriger Annahme eines illegalen Geheimnisses.

Sonstige Straftaten:

§ 120 Abs. 2	Gefangenenbefreiung,
§ 133 Abs. 3	Verwahrungsbruch.

Er / Sie hat einen Abdruck dieser Niederschrift, den “Verhaltenskodex gegen Korruption“ mit Erläuterungen und einen Abdruck der genannten Vorschriften sowie der geltenden Regelungen zur Annahme von Geschenken und Belohnungen erhalten.

Datum: _____
Ort: _____

_____ _____
(Unterschrift Verpflichtende/r) (Unterschrift Verpflichtete/r)

Musterklausel **Anlage 3**

Sinngemäße Anwendung der Korruptionspräventionsrichtlinie

„Der Zuwendungsempfänger [Name der Institution] wird verpflichtet, die als Anlage beigefügte Richtlinie der Bundesregierung zur Korruptionsprävention in der Bundesverwaltung vom 30. Juli 2004 sinngemäß anzuwenden. Um eine Zweckentfremdung der Mittel und die Beeinflussung des Geschäftsbetriebs durch Korruption zu vermeiden, trifft der Zuwendungsempfänger die geeigneten personellen und organisatorisch-administrativen Maßnahmen. Bei Anhaltspunkten auf Veruntreuung von Geldern, Korruptionsstraftaten oder anderen Verstößen gegen die Zweckbestimmung der Zuwendung ist das Bundesministerium …. zu informieren und sind Prüfungen zu ermöglichen.“

Musterklausel **Anlage 4**

Verhaltensstandards zur Korruptionsprävention

„Der Zuwendungsempfänger [Name der Institution] wird verpflichtet, die als Anlage beigefügten Verhaltensstandards einzuhalten. Um eine Zweckentfremdung der Mittel und die Beeinflussung des Geschäftsbetriebs durch Korruption zu vermeiden, trifft der Zuwendungsempfänger die geeigneten personellen und organisatorisch-administrativen Maßnahmen. Bei Anhaltspunkten auf Veruntreuung von Geldern, Korruptionsstraftaten oder anderen Verstößen gegen die Zweckbestimmung der Zuwendung ist das Bundesministerium …. zu informieren und sind Prüfungen zu ermöglichen.“

Verhaltensstandards zur Korruptionsprävention **noch Anlage 4**

Die folgenden Verhaltensstandards sollen Ihnen als Zuwendungsempfänger der Bundesrepublik Deutschland helfen, Korruption in Ihrem Bereich zu verhindern.

1. Wickeln Sie Ihre sämtlichen Geschäfte integer und verantwortlich ab. Gestalten Sie Ihre Geschäftsabläufe transparent, indem Sie beispielsweise Zuständigkeiten eindeutig regeln, (kurze) Berichte/Mustervermerke vorschreiben und Vorgänge dokumentieren und archivieren. Sorgen Sie dafür, dass Ihr Handeln und Ihre Beweggründe verständlich und nachvollziehbar sind.

2. Erfüllen Sie Ihre Vereinbarungen und Verträge und beachten Sie dabei die geltenden Rechtsvorschriften einschließlich derjenigen des Haushaltsrechts.

3. Stellen Sie fest, welche spezifischen Bereiche in Ihrem Aufgabenbereich (abstrakt) die größten Risiken für Korruption enthalten. Ergreifen Sie dort spezielle organisatorische Schutzmaßnahmen (z.B. Beachtung des Mehr-Augen-Prinzips; Verpflichtung der Beschäftigten, Gegenzeichnungen einzuholen; besonders sorgfältige Auswahl und Betreuung der Beschäftigten; Personal- oder Aufgabenrotation möglichst nach maximal fünf Jahren).

4. Verbieten Sie ausdrücklich das Anbieten, Geben, Annehmen oder Verlangen von Bestechungsgeldern in jeglicher Form, den Rückfluss von Teilen einer vertraglichen Zahlung („Kickback“) und das Nutzen anderer Wege, um Leistungen, auf die kein Anspruch besteht, zu erlangen oder zu erbringen.

5. Verbieten Sie ausdrücklich das Anbieten oder Annehmen von Geschenken, Bewirtungen und Vergünstigungen, soweit diese Handlungen oder Unterlassungen beeinflussen sollen und den Rahmen vernünftiger und angemessener Aufwendungen überschreiten.

6. Leisten Sie weder direkte noch indirekte Spenden an Parteien, Organisationen oder politisch tätige Einzelpersonen, um damit Vorteile für eigene Zwecke oder zugunsten von Angehörigen, Freunden, Partnern oder Bekannten zu erzielen; das gilt auch für Ihre Beschäftigten.

7. Unterstützen Sie die Einhaltung dieser Verhaltensstandards seitens der zuständigen Führungskräfte. Stellen Sie im Rahmen Ihrer Verantwortung si-

cher, vor allem bei der Ausübung Ihrer Kontrolltätigkeit, dass diese Verhaltensstandards eingehalten werden.

8. Informieren und sensibilisieren Sie Ihre Beschäftigten allgemein und gegebenenfalls zusätzlich bedarfsorientiert und arbeitsplatzbezogen. Sie und Ihre Beschäftigten - einschließlich der Führungskräfte -sollten die Möglichkeit zur Teilnahme an Schulungen nutzen.

9. Stellen Sie durch regelmäßige, konsequente Kontrollen sicher, dass die Maßnahmen zur Korruptionsprävention greifen.

10. Ermutigen Sie Ihre Beschäftigten bzw. die an einem Projekt mitwirkenden Personen, Anzeichen korrupten Verhaltens so früh wie möglich zu melden. Hieraus dürfen ihnen keine Nachteile erwachsen, wenn es sich um einen begründeten Verdacht handelt. Es ist sicherzustellen, dass vertrauliche Bedenken mitgeteilt und Zuwiderhandlungen / Verstöße angezeigt werden können.

11. Informieren Sie den Zuwendungsgeber (das für Sie zuständige Bundesministerium) bei Anhaltspunkten auf Veruntreuung von Geldern oder anderen auf Korruption beruhenden Handlungen.

12. Weisen Sie Ihre Beschäftigten ausdrücklich darauf hin, dass jede Form von Korruption verboten ist. Verpflichten Sie Ihre Beschäftigten auf die Einhaltung dieser Grundsätze.

13. Seien Sie Vorbild: Zeigen Sie durch Ihr Verhalten, dass Sie Korruption weder dulden noch unterstützen.

Signatures

Number of pages (including this one): 20

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

Bundesministerium des Innern

Richtlinie der Bundesregierung zur Korruptionsprävention in der Bundesverwaltung

Vom 30. Juli 2004

Nach Artikel 86 Satz 1 des Grundgesetzes wird folgende Richtlinie erlassen:

1 Anwendungsbereich

1.1 Die Maßnahmen aller Dienststellen des Bundes zur Korruptionsprävention bestimmen sich nach dieser Richtlinie; als Dienststellen des Bundes gelten die obersten Bundesbehörden, die Behörden der unmittelbaren und mittelbaren Bundesverwal- tung, die Gerichte des Bundes und Sondervermögen des Bundes. Die Vorschrift findet auch auf die Streitkräfte Anwendung; Einzelheiten regelt das Bundesministerium der Verteidigung.

1.2 Diese Richtlinie gilt sinngemäß auch für juristische Personen des öffentlichen oder privaten Rechts, an denen ausschließlich die Bundesrepublik Deutschland beteiligt ist.

1.3 Im Übrigen ist den jeweiligen organisatorischen und fachlichen Besonderheiten Rechnung zu tragen.

2 Feststellen und Analysieren besonders korruptionsgefährdeter Arbeitsgebiete

In allen Dienststellen des Bundes sind in regelmäßigen Abständen sowie aus gegebenem Anlass die besonders korruptionsgefährdeten Arbeitsgebiete festzustellen.
Für diese ist die Durchführung von Risikoanalysen zu prüfen. Je nach den Ergebnissen der Risikoanalyse ist zu prüfen, wie die Aufbau-, Ablauforganisation und/oder die Personalzuordnung zu ändern ist.

3 Mehr-Augen-Prinzip und Transparenz

3.1 Vor allem in besonders korruptionsgefährdeten Arbeitsgebieten ist das Mehr-Augen-Prinzip (Beteiligung bzw. Mitprüfung durch mehrere Beschäftigte oder Organisationseinheiten) sicherzustellen. Stehen dem Rechtsvorschriften oder unüberwindliche praktische Schwierigkeiten entgegen, kann die Mitprüfung auf Stichproben beschränkt werden oder es sind zum Ausgleich andere Maßnahmen der Korruptionsprävention (z. B. eine intensivere Dienst- und Fachaufsicht) vorzusehen.

3.2 Die Transparenz der Entscheidungen einschließlich der Entscheidungsvorbereitung ist sicherzustellen (z. B. durch eindeutige Zuständigkeitsregelung, Berichtswesen, IT-gestützte Vorgangskontrolle, genaue und vollständige verfahrensbegleitende Dokumentation).

4 Personal

4.1 Das Personal für besonders korruptionsgefährdete Arbeitsgebiete ist mit besonderer Sorgfalt auszuwählen.

4.2 In besonders korruptionsgefährdeten Bereichen ist die Verwendungsdauer des Personals grundsätzlich zu begrenzen; sie sollte in der Regel eine Dauer von fünf Jahren nicht überschreiten. Bei einer erforderlichen Verlängerung sind die Gründe aktenkundig zu machen.

5 Ansprechperson für Korruptionsprävention

5.1 Abhängig von Aufgabe und Größe der Dienststelle ist eine Ansprechperson für Korruptionsprävention zu bestellen. Sie kann auch für mehrere Dienststellen zuständig sein. Ihr können folgende Aufgaben übertragen werden:

a) Ansprechpartner bzw. Ansprechpartnerin für Beschäftigte und Dienststellenleitung, auch ohne Einhaltung des Dienstweges, sowie für Bürgerinnen und Bürger;
b) Beratung der Dienststellenleitung;
c) Aufklärung der Beschäftigten (z. B. durch regelmäßige Informationsveranstaltungen);
d) Mitwirkung bei der Fortbildung;
e) Beobachtung und Bewertung von Korruptionsanzeichen;
f) Mitwirkung bei der Unterrichtung der Öffentlichkeit über dienst- und strafrechtliche Sanktionen (Präventionsaspekt) unter Beachtung der Persönlichkeitsrechte der Betroffenen.

5.2 Werden der Ansprechperson Tatsachen bekannt, die den Verdacht einer Korruptionsstraftat begründen, unterrichtet sie die Dienststellenleitung und macht in diesem Zusammenhang Vorschläge zu internen Ermittlungen, zu Maßnahmen gegen Verschleierung und zur Mitteilung an die Strafverfolgungsbehörden. Die Dienststellenleitung veranlasst die zur Aufklärung des Sachverhalts erforderlichen Schritte.

5.3 Der Ansprechperson dürfen keine Disziplinarbefugnisse übertragen werden; in Disziplinarverfahren wegen Korruption wird sie nicht als Ermittlungsführer tätig.

5.4 Die Dienststellen haben die Ansprechperson zur Wahrnehmung ihrer Aufgaben rechtzeitig und

umfassend zu informieren, insbesondere bei korruptionsverdächtigen Vorfällen.

5.5 Bei der Wahrnehmung ihrer Aufgaben zur Korruptionsprävention ist die Ansprechperson weisungsunabhängig. Sie hat ein unmittelbares Vortragsrecht bei der Dienststellenleitung und darf wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden.

5.6 Die Ansprechperson hat über ihr bekannt gewordene persönliche Verhältnisse von Beschäftigten, auch nach Beendigung ihrer Amtszeit, Stillschweigen zu bewahren; dies gilt nicht gegenüber der Dienststellenleitung und der Personalverwaltung, wenn sie Tatsachen erfährt, die den Verdacht einer Korruptionsstraftat begründen. Personenbezogene Daten sind nach den Grundsätzen der Personalaktenführung zu behandeln.

6 Organisationseinheit zur Korruptionsprävention

Wenn Ergebnisse von Risikoanalysen oder besondere Anlässe es erfordern, sollte befristet oder auf Dauer eine gesonderte weisungsunabhängige Organisationseinheit zur Überprüfung und Bündelung der im jeweiligen Hause praktizierten Maßnahmen zur Korruptionsprävention eingerichtet werden; es besteht ein unmittelbares Vortragsrecht bei der Dienststellenleitung. Diese Aufgabe kann auch von der Innenrevision wahrgenommen werden. Bei Mängeln in der Korruptionsprävention unterrichtet diese Organisationseinheit die Dienststellenleitung und die Ansprechperson für Korruptionsprävention unmittelbar; sie soll Empfehlungen für geeignete Änderungen unterbreiten.

7 Sensibilisierung und Belehrung der Beschäftigten

7.1 Die Beschäftigten sind anlässlich des Diensteides oder der Verpflichtung auf Korruptionsgefahren aufmerksam zu machen und über die Folgen korrupten Verhaltens zu belehren. Die Belehrung ist zu dokumentieren. Hinsichtlich möglicher Korruptionsgefahren sind die Beschäftigten auch in der weiteren Folge zu sensibilisieren**.** Darüber hinaus soll ein „Verhaltenskodex gegen Korruption“ (siehe An- lage 1) allen Beschäftigten vermitteln, was sie insbesondere in besonders korruptionsgefährdeten Arbeitsgebieten oder Situationen zu beachten haben.

7.2 Bei Tätigkeiten in besonders korruptionsgefährdeten Arbeitsgebieten – auch bei einem Wechsel dorthin – sollen in regelmäßigen Abständen eine erneute Sensibilisierung und eine vertiefte arbeitsplatzbezogene Belehrung der Beschäftigten erfolgen.

8 Aus- und Fortbildung

Die Aus- und Fortbildungseinrichtungen nehmen das Thema „Korruptionsprävention“ in ihre Programme auf. Hierbei ist vor allem der Fortbildungsbedarf der Führungskräfte, der Ansprechpersonen für Korruptionsprävention, der Beschäftigten in besonders korruptionsgefährdeten Arbeitsgebieten und der Beschäftigten der in Nr. 6 genannten Organisationseinheiten zu berücksichtigen.

9 Konsequente Dienst- und Fachaufsicht

9.1 Die Vorgesetzten üben ihre Dienst- und Fachaufsicht konsequent aus („Leitfaden für Vorgesetzte und Behördenleitungen“; Anlage 2). Dies umfasst eine aktive vorausschauende Personalführung und -kontrolle.

9.2 In diesem Zusammenhang achten die Vorgesetzten auf Korruptionssignale. Sie sensibilisieren regelmäßig und bedarfsorientiert ihre Mitarbeiterinnen und Mitarbeiter für Korruptionsgefahren.

10 Unterrichtungen und Maßnahmen bei Korruptionsverdacht

10.1 Bei einem durch Tatsachen begründeten Verdacht einer Korruptionsstraftat hat die Dienststellenleitung unverzüglich die Staatsanwaltschaft und die oberste Dienstbehörde zu unterrichten; au- ßerdem sind behördeninterne Ermittlungen und vor- beugende Maßnahmen gegen eine Verschleierung einzuleiten.

10.2 Die obersten Bundesbehörden teilen jährlich dem Bundesministerium des Innern – auch für den jeweils nachgeordneten Bereich – in vorgegebener anonymisierter Form die Verdachtsfälle mit, in denen Verfahren eingeleitet wurden (untergliedert nach Bereich, Sachverhalt, eingeleiteten Maßnahmen) sowie den Ausgang der Verfahren, die im Berichtsjahr abgeschlossen wurden**.**

11 Leitsätze für die Vergabe

11.1 Wettbewerb

Der Grundsatz der öffentlichen Ausschreibung bzw. des offenen Verfahrens hat im Rahmen der Korruptionsprävention besondere Bedeutung.
Bei der Vergabe öffentlicher Aufträge ist regelmäßig im Rahmen der Dienst- und Fachaufsicht zu prüfen, ob unzulässige Einflussfaktoren vorgelegen haben.

11.2 Grundsätzliche Trennung von Planung, Vergabe und Abrechnung

Bei der Vergabe von öffentlichen Aufträgen nach den haushalts- und vergaberechtlichen Bestimmun- gen sind Vorbereitung, Planung und Bedarfsbeschreibung einerseits und die Durchführung des Vergabeverfahrens andererseits sowie möglichst auch die spätere Abrechnung grundsätzlich organisatorisch zu trennen**.**

11.3 Wettbewerbsausschluss

Die Dienststellen prüfen, ob schwere Verfehlungen von Bietern bzw. Bieterinnen oder Bewerbern bzw. Bewerberinnen vorliegen, die ihre Zuverlässigkeit in Frage stellen und die zum Ausschluss vom Wettbewerb führen können.
Eine solche schwere Verfehlung liegt insbesondere vor, wenn eine der genannten Personen demjenigen, der mit der Vorbereitung oder Durchführung eines Vergabeverfahrens befasst ist, einen Vorteil für diesen oder einen Dritten anbietet, verspricht oder gewährt.

12 Antikorruptionsklausel, Verpflichtung von Auftragnehmern oder Auftragnehmerinnen nach dem Verpflichtungsgesetz

12.1 Bei der Vergabe von öffentlichen Aufträgen sind in geeigneten Fällen Antikorruptionsklauseln vorzusehen.

12.2 Wirken private Unternehmen bei der Ausführung von Aufgaben der öffentlichen Hand mit, sind die einzelnen Beschäftigten dieser Unternehmen – soweit erforderlich – nach dem Verpflichtungsgesetz auf die gewissenhafte Erfüllung ihrer Obliegenheiten aus dem Auftrag zu verpflichten. Ein entsprechender Hinweis ist bereits in die jeweilige Ausschreibung aufzunehmen (einschließlich der Einforderung einer Bereitschaftserklärung). Den genannten Personen sind der „Verhaltenskodex gegen Korruption“ (siehe Anlage 1) und ein Abdruck der gelten- den Regelungen zur Annahme von Belohnungen und Geschenken auszuhändigen.

13 Zuwendungen zu Gemeinschaftsveranstaltungen und Gemeinschaftseinrichtungen; Sponsoring

Für die Annahme von Geld-, Sach- oder Dienstleistungen durch Private (Sponsoren) an eine oder mehrere Dienststellen des Bundes gilt die Allgemeine Verwaltungsvorschrift der Bundesregierung zur Förderung von Tätigkeiten des Bundes durch Leistungen Privater (Sponsoring, Spenden und sonstige Schenkungen) vom 7. Juli 2003 (BAnz. S. 14906).

14 Zuwendungsempfänger

14.1 Für Zuwendungen des Bundes im Rahmen institutioneller Förderungen ist der Zuwendungsempfänger durch besondere Nebenbestimmungen im Zuwendungsbescheid zu verpflichten, diese Richtlinie sinngemäß anzuwenden, wenn ihm durch Haushaltsrecht die Anwendung des Vergaberechts aufgegeben worden ist (Höhe der Zuwendung oder bei Finanzierung durch mehrere Stellen der Gesamtbetrag der Zuwendung mehr als 100.000 €). Bei Zuwendungsverträgen ist die entsprechende Anwendung der Richtlinie vertraglich zu vereinbaren.

14.2 Mit institutionellen Zuwendungsempfängern im Ausland sind vertraglich Grundsätze zur Korruptionsprävention zu vereinbaren.

15 Besondere Maßnahmen

Soweit erforderlich, können die Dienststellen weitere über die Richtlinie hinausgehende Maßnahmen treffen.

16 Inkrafttreten

Diese Richtlinie tritt am Tage nach ihrer Veröffentlichung im Bundesanzeiger in Kraft. Gleichzeitig tritt die Richtlinie vom 17. Juni 1998 (BAnz Nr. 127, S. 9665) außer Kraft.

Berlin, den 30. Juli 2004
O 4 – 634 140-15/1

Der Bundesminister des Innern

S c h i l y

Anlage 1

Verhaltenskodex gegen Korruption

Dieser Verhaltenskodex soll die Beschäftigten auf Gefahrensituationen hinweisen, in denen sie ungewollt in Korruption verstrickt werden können. Weiterhin soll er die Beschäftigten zur pflichtgemäßen und gesetzestreuen Erfüllung ihrer Aufgaben anhal- ten und ihnen die Folgen korrupten Verhaltens vor Augen führen:

Daher:

1. **Seien Sie Vorbild: Zeigen Sie durch Ihr Verhalten, dass Sie Korruption weder dulden noch unterstützen.**

2. **Wehren Sie Korruptionsversuche sofort ab und informieren Sie unverzüglich die Ansprechperson für Korruptionsprävention und Ihre Vorgesetzte oder Ihren Vorgesetz- ten.**

3. **Vermuten Sie, dass jemand Sie um eine pflichtwidrige Bevorzugung bitten will, so ziehen Sie einen Kollegen oder eine Kollegin als Zeugen oder Zeugin hinzu.**

4. **Arbeiten Sie so, dass Ihre Arbeit jederzeit überprüft werden kann.**

5. **Trennen Sie strikt Dienst- und Privatleben. Prüfen Sie, ob Ihre Privatinteressen zu einer Kollision mit Ihren Dienstpflichten führen.**

6. **Unterstützen Sie Ihre Dienststelle bei der Entdeckung und Aufklärung von Korruption. Informieren Sie die Ansprechperson für Korruptionsprävention und Ihre Vorgesetzte oder Ihren Vorgesetzten bei konkreten Anhaltspunkten für korruptes Verhalten.**

7. **Unterstützen Sie Ihre Dienststelle beim Erkennen fehlerhafter Organisationsstrukturen, die Korruption begünstigen.**

8. **Lassen Sie sich zum Thema Korruptionsprävention aus- und fortbilden.**

9. **Und was tun, wenn Sie sich bereits verstrickt haben?**
   Befreien Sie sich von der ständigen Angst vor Entdeckung! Machen Sie reinen Tisch! Offenbaren Sie sich aus eigenem Antrieb und führen Ihre Angaben zur vollständigen Aufklärung des Sachverhaltes, kann dies sowohl bei der Strafzumessung als auch bei dienstrechtlichen Reaktionen mildernd berücksichtigt werden.

zu 1.
Korruption in der öffentlichen Verwaltung könnte besser verhindert werden, wenn sich jeder zum Ziel setzt, Korruption zu bekämpfen. Dies entspricht auch den Pflichten, die Beschäftigte bei der Einstellung gegenüber dem Dienstherrn bzw. dem Arbeitgeber übernommen haben:
Beschäftigte haben sich bei ihrer Einstellung verpflichtet, das Grundgesetz für die Bundesrepublik Deutschland und die geltenden Gesetze zu wahren und ihre Aufgaben gewissenhaft zu erfüllen. Be- schäftigte haben sich so zu verhalten, wie es von Angehörigen des öffentlichen Dienstes erwartet wird und sich darüber hinaus durch ihr gesamtes Verhal- ten zur freiheitlich-demokratischen Grundordnung im Sinne des Grundgesetzes zu bekennen. Alle Beschäf- tigten haben ihre Aufgaben daher unparteiisch und gerecht zu erfüllen.

Korruptes Verhalten widerspricht diesen Verpflichtungen und schädigt das Ansehen des öffentlichen Dienstes. Es zerstört das Vertrauen in die Unparteilichkeit und Objektivität der Staatsverwaltung und damit die Grundlagen für das Zusammenleben in einem staatlichen Gemeinwesen.

Alle Beschäftigten haben daher die Aufgabe, durch ihr Verhalten Vorbild für alle anderen, für Vorge- setzte und für Bürger und Bürgerinnen zu sein.

zu 2.
Bei Außenkontakten, z. B. mit Personen der Auftragnehmerseite oder der antragstellenden Seite oder bei Kontrolltätigkeiten, müssen Sie von Anfang an klare Verhältnisse schaffen und jeden Korruptionsversuch sofort abwehren. Es darf nie der Eindruck entstehen, dass Sie für „kleine Geschenke“ offen sind. Scheuen Sie sich nicht, ein Geschenk zurückzuweisen oder es zurückzusenden – mit der Bitte um Verständnis für die für Sie geltenden Regeln.

Arbeiten Sie in einem Verwaltungsbereich, der sich mit der Vergabe von öffentlichen Aufträgen beschäftigt, so seien Sie besonders sensibel für Versuche Dritter, Einfluss auf Ihre Entscheidung zu nehmen. In diesem Bereich gibt es die meisten Korruptionshandlungen.

Halten Sie sich daher streng an Recht und Gesetz und beachten Sie die Richtlinien zum Verbot der Annahme von Belohnungen oder Geschenken.

Wenn Sie von Dritten um eine zweifelhafte Gefälligkeit gebeten worden sind, so informieren Sie unverzüglich Ihre Vorgesetzte oder Ihren Vorgesetzten und die Ansprechperson für Korruptionsprävention. Das hilft zum einen, selbst jeglichem Korruptionsverdacht zu entgehen, zum anderen aber auch, u. U. rechtliche Maßnahmen gegen Dritte einleiten zu können. Wenn Sie einen Korruptionsversuch zwar selbst abwehren, ihn aber nicht offenbaren, so wird sich Ihr Gegenüber an einen anderen wenden und es bei ihm versuchen. Schützen Sie daher auch Ihre Kollegen und Kolleginnen durch konsequentes Offenlegen von Korruptionsversuchen Außenstehender. Alle Beschäftigten (Vorgesetzte, Mitarbeiterinnen und Mitarbeiter) müssen an einem Strang ziehen, um einheitlich und glaubhaft aufzutreten.

zu 3.
Manchmal steht Ihnen ein Gespräch bevor, bei dem Sie vermuten, dass ein zweifelhaftes Ansinnen an Sie gestellt und dieses nicht leicht zurückzuweisen sein wird. Hier hilft oftmals auch eindeutige Distanzierung nicht. In solchen Fällen sollten Sie sich der Situation nicht allein stellen, sondern einen anderen zu dem Gespräch hinzubitten. Sprechen Sie vorher mit ihm und bitten Sie ihn, auch durch sein Verhalten jeglichen Korruptionsversuch abzuwehren.

zu 4.
Ihre Arbeitsweise sollte transparent und für jeden nachvollziehbar sein.
Da Sie Ihren Arbeitsplatz in der Regel wieder verlassen werden (Übertragung neuer Aufgaben, Versetzung) oder auch einmal kurzfristig ausfallen (Krankheit, Urlaub), sollten Ihre Arbeitsvorgänge schon deshalb so transparent sein, dass sich jederzeit eine Sie vertretende Person einarbeiten kann. Die transparente Aktenführung hilft Ihnen aber auch, sich bei Kontrollvorgängen vor dem ausgesprochenen oder unausgesprochenen Vorwurf der Unredlichkeit zu schützen. "Nebenakten" sollten Sie vermeiden, um jeden Eindruck von Unredlichkeit von vornherein auszuschließen. Handakten sind nur zu führen, wenn es für die Erledigung der Arbeit unumgänglich ist.

zu 5.
Korruptionsversuche werden oftmals gestartet, indem Dritte den dienstlichen Kontakt auf Privatkontakte ausweiten. Es ist bekanntermaßen besonders schwierig, eine „Gefälligkeit“ zu verweigern, wenn man sich privat hervorragend versteht und man selber oder die eigene Familie Vorteile und Vergünstigungen erhält (Konzertkarten, verbilligter gemeinsamer Urlaub, Einladungen zu teuren Essen, die man nicht erwidern kann usw.). Bei privaten Kontakten sollten Sie daher von Anfang an klarstellen, dass Sie streng zwischen Dienst- und Privatleben trennen müssen, um nicht in den Verdacht der Vorteilsannahme zu geraten.

Diese strenge Trennung zwischen privaten Interessen und dienstlichen Aufgaben müssen Sie ohnehin – unabhängig von einer Korruptionsgefahr – bei Ihrer gesamten dienstlichen Tätigkeit beachten. Ihre Dienststelle, jeder Bürger und jede Bürgerin haben Anspruch auf Ihr faires, sachgemäßes, unparteiisches Verhalten. Prüfen Sie daher bei jedem Verfahren, für das Sie mitverantwortlich sind, ob Ihre privaten Interessen oder solche Ihrer Angehörigen oder z. B. auch von Organisationen, denen Sie verbunden sind, zu einer Kollision mit Ihren hauptberuflichen Verpflichtungen führen können. Vermeiden Sie jeden bösen Schein möglicher Parteilichkeit. Sorgen Sie dafür, dass Sie niemandem befangen erscheinen, auch nicht durch „atmosphärische“ Einflussnahmen von interessierter Seite.
Erkennen Sie bei einer konkreten dienstlichen Aufgabe eine mögliche Kollision zwischen Ihren dienstlichen Pflichten und Ihren privaten Interessen oder den Interessen Dritter, denen Sie sich verbunden fühlen, so unterrichten Sie darüber Ihren Vorgesetz- ten oder Ihre Vorgesetzte, damit angemessen reagiert werden kann (z. B. Befreiung von Tätigkeiten im konkreten Einzelfall).

Auch bei von Ihnen ausgeübten oder angestrebten Nebentätigkeiten muss eine klare Trennung zwischen der Arbeit und der Nebentätigkeit bleiben. Persönliche Verbindungen, die sich aus der Nebentätigkeit ergeben, dürfen die hauptberufliche Tätigkeit nicht beeinflussen. Verzichten Sie im Einzelfall auf die Nebentätigkeit.
Bedenken Sie außerdem, dass bei Ausübung genehmigungspflichtiger, aber nicht genehmigter Nebentätigkeiten dienst- bzw. arbeitsrechtliche Konsequenzen drohen; dasselbe gilt bei Versäumnis von Anzeigepflichten.

Unabhängig davon schadet es früher oder später Ihrem Ansehen – und damit dem Ansehen des ge- samten öffentlichen Dienstes – wenn Sie im Kon- fliktfall Ihren privaten Interessen den Vorrang gege- ben haben. Das gilt in besonderem Maße, wenn Sie an einflussreicher Stelle tätig sind. Achten Sie in diesem Fall besonders darauf, nur jene Konditionen in Anspruch zu nehmen, die für vergleichbare Umstände abstrakt geregelt sind.

zu 6.
Korruption kann nur verhindert und bekämpft werden, wenn sich jeder verantwortlich fühlt und alle als gemeinsames Ziel die "korruptionsfreie Dienststelle" verfolgen. Das bedeutet zum einen, dass alle Beschäftigten im Rahmen ihrer Aufgaben dafür sorgen müssen, dass Außenstehende keine Möglichkeit zur

unredlichen Einflussnahme auf Entscheidungen haben.
Das bedeutet aber auch, dass korrupte Beschäftigte nicht aus falsch verstandener Solidarität oder Loyalität gedeckt werden dürfen. Hier haben alle die Verpflichtung, zur Aufklärung von strafbaren Handlungen beizutragen und die eigene Dienststelle vor Schaden zu bewahren. Ein "schwarzes Schaf" verdirbt die ganze Herde. Beteiligen Sie sich deshalb nicht an Vertuschungsversuchen.

Für jede Dienststelle gibt es eine Ansprechperson für Korruptionsprävention. Sie sollten sich nicht scheuen, mit ihr zu sprechen, wenn das Verhalten von anderen Beschäftigten Ihnen konkrete und nachvollziehbare Anhaltspunkte dafür gibt, dass sie bestechlich sein könnten. Die Ansprechperson wird Ihren Wunsch auf Stillschweigen berücksichtigen und dann entscheiden, ob und welche Maßnahmen zu treffen sind. Ganz wesentlich ist allerdings, dass Sie einen Verdacht nur dann äußern, wenn Sie nachvollziehbare Hinweise dafür haben. Es darf nicht dazu kom- men, dass andere angeschwärzt werden, ohne dass ein konkreter Anhaltspunkt vorliegt.

zu 7.
Oftmals führen lang praktizierte Verfahrensabläufe dazu, dass sich Nischen bilden, in denen Korruption besonders gut gedeihen kann. Das können Verfahren sein, bei denen nur eine Person allein für die Vergabe von Vergünstigungen verantwortlich ist. Das können aber auch unklare Arbeitsabläufe sein, die eine Überprüfung erschweren oder verhindern.
Hier kann meistens eine Änderung der Organisationsstrukturen Abhilfe schaffen. Daher sind alle Beschäftigten aufgefordert, entsprechende Hinweise an die Organisatoren zu geben, um zu klaren und transparenten Arbeitsabläufen beizutragen.
Auch innerhalb von Arbeitseinheiten müssen Arbeitsabläufe so transparent gestaltet werden, dass Korruption gar nicht erst entstehen kann.

Ein weiteres Mittel, um Gefahrenpunkte wirksam auszuschalten, ist das Rotieren von Personal. In besonders korruptionsgefährdeten Bereichen ist daher dieses Personalführungsinstrument verstärkt einzusetzen. Dazu ist die Bereitschaft der Beschäftigten zu einem regelmäßigen Wechsel – in der Regel sollte die Verwendungsdauer fünf Jahre nicht überschreiten – der Aufgaben zwingend erforderlich, auch wenn dies im Regelfall mit einem höheren Arbeitsanfall (Einarbeitungszeit!) verbunden ist.

zu 8.
Wenn Sie in einem besonders korruptionsgefährdeten Bereich tätig sind, nutzen Sie die Angebote der Dienststelle, sich über Erscheinungsformen, Gefahrensituationen, Präventionsmaßnahmen, strafrechtliche sowie dienst- oder arbeitsrechtliche Konsequenzen von Korruption aus- und fortbilden zu lassen. Dabei werden Sie lernen, wie Sie selbst Korruption verhindern können und wie Sie reagieren müssen, wenn Sie korrumpiert werden sollen oder Korruption in Ihrem Arbeitsumfeld entdecken. Aus- und Fortbildung werden Sie sicher machen, mit dem Thema Korruption in der richtigen, gesetzestreuen Weise umzugehen.

Anlage 2

Leitfaden für

Vorgesetzte und Behördenleitungen

I.

Als Vorgesetzte und Behördenleitungen haben Sie eine Vorbildfunktion und Fürsorgepflicht für die Ihnen unterstellten Beschäftigten.
Ihr Verhalten, aber auch Ihre Aufmerksamkeit sind von großer Bedeutung für die Korruptionsprävention. Sie sollten daher eine aktive, vorausschauende Personalführung und -kontrolle praktizieren. Insbesondere sollten Sie klare Zuständigkeitsregelungen und transparente Aufgabenbeschreibungen für die Mitarbeiterinnen und Mitarbeiter sowie eine angemessene Kontrolldichte sicherstellen.

Schwachstellen und Einfallstore für Korruption sind z. B.:

1. mangelhafte Dienst- und Fachaufsicht;
2. blindes Vertrauen gegenüber langjährigen Beschäftigten und spezialisierten Beschäftigten;
3. charakterliche Schwächen von Beschäftigten in korruptionsgefährdeten Bereichen;
4. negatives Vorbild von Vorgesetzten bei der Annahme von Präsenten;
5. ausbleibende Konsequenzen nach aufgedeckten Manipulationen; dadurch keine Abschreckung.

Sie können solchen Schwachstellen durch folgende Maßnahmen begegnen:

1. Belehrung und Sensibilisierung

Sprechen Sie mit Ihren Beschäftigten in regelmäßigen Abständen anhand des „Verhaltenskodex gegen Korruption“ über die Verpflichtungen, die sich aus dem Verbot der Annahme von Belohnungen und Geschenken und aus den Vorschriften zur Vermeidung von Interessenkollisionen ergeben.

2. Organisatorische Maßnahmen (im Rahmen Ihrer Befugnisse)

Achten Sie auf klare Definition und ggf. auf Einschränkungen der Entscheidungsspielräume.

Erörtern Sie die Delegationsstrukturen, die Grenzen der Ermessensspielräume und die Notwendigkeit von Mitzeichnungspflichten.

Achten Sie in besonders korruptionsgefährdeten Arbeitsgebieten auf eine Flexibilisierung der Vorgangsbearbeitung nach numerischen oder Buchstabensystemen durch

a) kritische Überprüfung der Sachbearbeitung nach diesen Systemen;
b) Einzelzuweisung nach dem Zufallsprinzip oder
c) durch wiederholten Wechsel der Nummern- oder Buchstabenzuständigkeiten einzelner Personen.

Realisieren Sie – wenn irgend möglich – das Mehr-Augen-Prinzip auch in Ihrem Verantwortungsbereich. Eventuell bietet sich die Bildung von Arbeitsteams bzw. -gruppen an. Prüfen Sie, ob die Begleitung einzelner Beschäftigter durch weitere Bedienstete zu Ortsterminen, Kontrollen vor Ort usw. oder die Einrichtung von „gläsernen Büros“ für die Abwicklung des Besucherverkehrs geboten ist, damit Außenkontakte der Dienststelle nur nach dem Mehr-Augen-Prinzip wahrgenommen werden. Wo sich das wegen der tatsächlichen Umstände nicht realisieren lässt, organisieren Sie Kontrollen – in nicht zu großen zeitlichen Abständen.

Setzen Sie personalwirtschaftliche Instrumente insbesondere bei Tätigkeiten mit schnell erlernbaren Fachkenntnissen konsequent ein:

1. In besonders korruptionsgefährdeten Bereichen in der Regel Rotation nach einem Zeitraum von 5 Jahren.
2. Ein Verzicht auf Umsetzung im Ausnahmefall – z. B. bei Tätigkeiten mit langfristig erworbenem Sachverstand – erfordert eine schriftliche Begründung und eine besonders gründliche Kontrolle des Arbeitsbereichs durch Vorgesetzte.

Ist in Ihrer Dienststelle die Zweierbelegung von Diensträumen nicht ungewöhnlich, so nutzen Sie dies ebenfalls zur Korruptionsprävention in besonders korruptionsgefährdeten Arbeitsgebieten, z. B. durch sporadischen Wechsel der Raumbesetzungen (auch ohne Aufgabenänderung für die Beschäftigten).

3. Fürsorge

In besonders korruptionsgefährdeten Arbeitsgebieten erfordert Korruptionsprävention auch eine erhöhte Fürsorge für Ihre Beschäftigten.

a) Berücksichtigen Sie stets die erhöhte Gefährdung Einzelner.
b) Auch der ständige Dialog ist ein Mittel der Fürsorge.
c) Beachten Sie dienstliche und private Probleme Ihrer Beschäftigten.
d) Sorgen Sie für Abhilfe z. B. durch Entbindung eines Mitarbeiters oder einer Mitarbeiterin von Aufgaben, wenn Ihnen Interessenkollisionen durch Nebentätigkeiten oder durch Tätigkeiten von Angehörigen bekannt werden.
e) Besondere Wachsamkeit ist bei erkennbarer Überforderung oder Unterforderung Einzelner geboten.
f) Ihre erhöhte Aufmerksamkeit verlangt es, wenn Ihnen persönliche Schwächen (z. B. Suchtprobleme, Hang zu teuren, schwer zu

finanzierenden Hobbys) oder eine Überschuldung bekannt werden; Beschäftigte, deren wirtschaftliche Verhältnisse nicht geordnet sind, sollen im Beschaffungswesen sowie auf Dienstposten, auf denen sie der Gefahr einer unlauteren Beeinflussung durch Dritte besonders ausgesetzt sind, nicht eingesetzt werden.

g) Schließlich müssen Sie auch bei offen vorgetragener Unzufriedenheit mit dem Dienstherrn besonders wachsam sein und versuchen, dem entgegenzuwirken.

4. Aufsicht; Führungsstil

Machen Sie sich bewusst, dass es bei Korruption keinen beschwerdeführenden Geschädigten gibt und Korruptionsprävention deshalb wesentlich von Ihrer Sensibilität und der Sensibilisierung Ihrer Beschäftigten abhängt. Sie erfordert aber auch Ihre Dienst- und Fachaufsicht – ohnehin Ihre Kernpflicht als Vorgesetzter. Ein falsch verstandener kooperativer Führungsstil oder eine „laissez-faire"-Haltung können in besonders korruptionssensiblen Bereichen verhängnisvoll sein. Versuchen Sie deshalb,

a) die Vorgangskontrolle zu optimieren, indem Sie z. B. Kontrollmechanismen (Wiedervorlagen o. ä.) in den Geschäftsablauf einbauen,
b) das Abschotten oder eine Verselbständigung einzelner Beschäftigter zu vermeiden,
c) dem Auftreten von Korruptionsindikatoren besondere Wachsamkeit zu schenken,
d) stichprobenweise das Einhalten vorgegebener Ermessensspielräume zu überprüfen,
e) die Akzeptanz des Verwaltungshandelns durch Gespräche mit "Verwaltungskunden" zu ermitteln.

Nutzen Sie das Fortbildungsangebot bei Lehrgängen zur Korruptionsprävention.

II.

1. Anzeichen für Korruption, Warnsignale

Trotzdem ist Korruption nicht auszuschließen. Nach dem Ergebnis einer vom Bundeskriminalamt durchgeführten Expertenbefragung[1] ist korruptes Verhalten häufig mit Verhaltensweisen verbunden, die als Korruptionssignale gewertet werden können. Diese Wertung ist aber mit Unwägbarkeiten verbunden, weil einige der Indikatoren als neutral oder sogar positiv gelten, obwohl sie sich nachträglich als verlässliche Signale erwiesen haben.

Keiner der Indikatoren ist ein „Nachweis" für Korruption. Wenn Ihnen aber aufgrund von Äußerungen oder Beobachtungen ein Verhalten auffällig erscheint, müssen Sie prüfen, ob das Auftreten eines Indikators zusammen mit den Umfeldbedingungen eine Korruptionsgefahr anzeigt.

1.1 Neutrale Indikatoren

a) auffallender und unerklärlich hoher Lebensstandard; aufwändiger Lebensstil; Vorzeigen von Statussymbolen;
b) auffällige private Kontakte zwischen Beschäftigten und Dritten (z. B. Einladungen, Nebentätigkeiten, Berater- oder Gutachterverträge, Kapitalbeteiligungen);
c) unerklärlicher Widerstand gegen eine Aufgabenänderung oder eine Umsetzung, insbesondere wenn sie mit einer Beförderung bzw. Gehaltsaufbesserung oder zumindest der Aussicht darauf verbunden wäre;
d) Ausübung von Nebentätigkeiten ohne entsprechende Genehmigung bzw. Anzeige;
e) atypisches, nicht erklärbares Verhalten (z. B. aufgrund eines bestehenden Erpressungsverhältnisses bzw. schlechten Gewissens); aufkommende Verschlossenheit; plötzliche Veränderungen im Verhalten gegenüber Kollegen und Kolleginnen und Vorgesetzten;
f) abnehmende Identifizierung mit dem Dienstherrn oder den Aufgaben;
g) soziale Probleme (Alkohol-, Drogen- oder Spielsucht u. ä.);
h) Geltungssucht, Prahlen mit Kontakten im dienstlichen und privaten Bereich;
i) Inanspruchnahme von Vergünstigungen Dritter (Sonderkonditionen beim Einkauf, Freihalten in Restaurants, Einladungen zu privaten oder geschäftlichen Veranstaltungen von „Verwaltungskunden");
j) auffallende Großzügigkeit von Unternehmen (z. B. Sponsoring).

1.2 Alarmindikatoren

Außer diesen eher neutralen gibt es solche Indikatoren, die nach den Erfahrungen des BKA charakteristisch für die Verwaltungskorruption sind und deshalb als „Alarmindikatoren" eingestuft werden müssen.

Dienststelleninterne Indikatoren:

a) Umgehen oder „Übersehen" von Vorschriften; Häufung „kleiner Unregelmäßigkeiten"; Abweichungen zwischen tatsächlichem Vorgangsablauf und späterer Dokumentation;
b) mangelnde Identifikation mit dem Dienstherrn oder den Aufgaben;
c) ungewöhnliche Entscheidungen ohne nachvollziehbare Begründung;
d) unterschiedliche Bewertungen und Entscheidungen bei Vorgängen mit gleichem Sachverhalt und verschiedenen antragstellenden Personen; Missbrauch von Ermessensspielräumen;
e) Erteilung von Genehmigungen (z. B. mit Befreiung von Auflagen) unter Umgehung anderer zuständiger Stellen;

[1] Vgl. BKA Forschungsreihe „Korruption - hinnehmen oder handeln? S. 151 – 160; Wiesbaden 1995

f) gezielte Umgehung von Kontrollen, Abschottung einzelner Aufgabenbereiche;
g) Verheimlichen von Vorgängen;
h) auffallend kurze Bearbeitungszeiten bei einzelnen begünstigenden Entscheidungen;
i) Parteinahme für bestimmte antragstellende oder bietende Personen;
j) Verharmlosung des Sparsamkeitsprinzips;
k) Versuche der Beeinflussung von Entscheidungen bei Aufgaben, die nicht zum eigenen Zuständigkeitsbereich gehören und bei denen Drittinteressen von Bedeutung sind;
l) stillschweigende Duldung von Fehlverhalten, insbesondere bei rechtswidrigem Verhalten;
m) fehlende oder unzureichende Vorgangskontrolle dort, wo sie besonders notwendig wäre; zu schwach ausgeprägte Dienst- und Fachaufsicht;
n) Ausbleiben von Reaktionen auf Verdachtsmomente oder Vorkommnisse;
o) zu große Aufgabenkonzentration auf eine Person.

Indikatoren im Bereich der Außenkontakte:

a) auffallend entgegenkommende Behandlung von antragstellenden Personen;
b) Bevorzugung beschränkter Ausschreibungen oder freihändiger Vergaben; auch Splitten von Aufträgen, um freihändige Vergaben zu ermöglichen; Vermeiden des Einholens von Vergleichsangeboten;
c) erhebliche bzw. wiederholte Überschreitung der vorgesehenen Auftragswerte;
d) Beschaffungen zum marktunüblichen Preis; unsinnige Anschaffungen; Abschluss langfristiger Verträge ohne transparenten Wettbewerb mit für die Dienststelle ungünstigen Konditionen;
e) auffallend häufige „Rechenfehler“, Nachbesserungen in Leistungsverzeichnissen;
f) Eingänge in Vergabesachen ohne Eingangsstempel (Eingang „über die persönliche Schiene“);
g) aufwändige Nachtragsarbeiten;
h) Nebentätigkeiten von Beschäftigten oder Tätigkeit ihrer Angehörigen für Firmen, die gleichzeitig Auftragnehmer oder Antragsteller der öffentlichen Verwaltung sind;
i) „kumpelhafter“ Umgangston oder auffallende Nachgiebigkeit bei Verhandlungen mit Unternehmen;
j) Ausspielen von (vermeintlichen) Machtpositionen durch Unternehmen;
k) häufige „Dienstreisen“ zu bestimmten Firmen (auffallend insbesondere dann, wenn eigentlich nicht erforderliche Übernachtungen anfallen);
l) „permanente Firmenbesuche“ von Unternehmen in der Dienststelle (bei bestimmten Entscheidungsträgern oder Sachbearbeitern) und Vorsprache bestimmter Unternehmen nur dann, wenn Beschäftigte „ihrer“ Dienststelle anwesend sind;
m) Ausbleiben von Konflikten mit Unternehmen bzw. Antragstellern/Antragstellerinnen dort, wo sie üblicherweise vorkommen.

Nach der Forschungsarbeit des BKA macht die Liste dieser Indikatoren deutlich, dass die Merkmale insbesondere dann von Interesse sein können, wenn sich etwas außerhalb der üblichen Norm bewegt („unerklärlich“, „nicht nachvollziehbar“, „sich plötzlich verändernd“, „auffallend“). Als häufiges und hervorstechendes Warnsignal hebt es den typischerweise aufwändigen bzw. ungewöhnlich hohen Lebensstandard von Beschäftigten mit „Nebenverdiensten“ heraus, wozu auch das Vorzeigen entsprechender Statussymbole gehört. Understatement sei in diesen Täterkreisen weniger zu erwarten.

Als Warnsignale bezeichnen die vom BKA befragten Experten ferner Andeutungen im Kollegenkreis, Gerüchte von außen sowie anonyme Hinweise (z. B. von benachteiligten und dadurch in finanzielle Schwierigkeiten geratenen Unternehmen). Diese Signale würden noch deutlicher, wenn sie sich häufen und auf bestimmte Personen oder Aufgabenbereiche konzentrieren. Allerdings sei eine ständige Gewichtung und Analyse der „Gerüchteküche“ unabdingbar, um Missbrauch auszuschließen. Andererseits haben anonyme Hinweise vielfach den Anlass zu Ermittlungen gegeben, durch die dann tatsächlich Korruption aufgedeckt wurde.

2. Verdacht

Bei konkreten und nachvollziehbaren Anhaltspunkten für einen Korruptionsverdacht müssen Sie sich unverzüglich mit der Ansprechperson für Korruptionsprävention beraten und die Personalverwaltung bzw. Behördenleitung informieren. Eventuell aber erfordern die Umstände auch, dass Sie selbst sofort geeignete Maßnahmen gegen eine Verschleierung ergreifen. Infrage kommen z. B.

a) der Entzug bestimmter laufender oder abgeschlossener Vorgänge,
b) das Verbot des Zugangs zu Akten,
c) die Sicherung des Arbeitsraumes, der Aufzeichnungen mit dienstlichem Bezug oder der Arbeitsmittel (z. B. Computer und Dis- ketten o. ä.).

Das Maß und der Umfang der gebotenen Maßnahmen können sich nur nach den Umständen des Einzelfalles richten.

Bedenken Sie, dass Korruption kein „Kavaliersdelikt“ und Vertuschen auch Ihrem Ansehen schädlich ist.

Bei Verletzung Ihrer Pflichten können Sie sich eines Dienstvergehens schuldig und strafbar machen.

Signatures

Number of pages (including this one): 10

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

Bundesministerium
der Verteidigung

A-2100/1

Zentrale Dienstvorschrift

Umsetzung der „Richtlinie der Bundesregierung zur Korruptionsprävention in der Bundesverwaltung“

Zweck der Regelung:	Weiterentwicklung zentraler Vorgaben zur Korruptionsprävention. Umsetzung der Empfehlungen des BMI zur Richtlinie der Bundesregierung. Anpassung/Ergänzung/Aufhebung von Regelungen.
Herausgegeben durch:	Bundesministerium der Verteidigung
Beteiligte Interessenvertretungen:	Hauptpersonalrat und Gesamtvertrauenspersonenausschuss
Gebilligt durch:	Staatssekretär Hoofe
Herausgebende Stelle:	BMVg R II 1
Geltungsbereich:	Geschäftsbereich des Bundesministeriums der Verteidigung
Einstufung:	Offen
Einsatzrelevanz:	Ja
Berichtspflichten:	Ja
Gültig ab:	21.05.2014
Frist zur Überprüfung:	30.04.2019
Version:	1
Ersetzt/hebt auf:	VMBl 2006 S.25-28, VMBl 2006 S. 29
Aktenzeichen:	75-70-00/004/03
Identifikationsnummer:	A.21001/1I

Inhaltsverzeichnis

1 Anwendungsbereich 5
1.1 Auszug aus Nr. 1 der Richtlinie 5
1.2 Durchführungsbestimmungen 5
2 Besonders korruptionsgefährdete Arbeitsgebiete 7
2.1 Auszug aus Nr. 2 der Richtlinie 7
2.2 Durchführungsbestimmungen 7
3 Mehr-Augen-Prinzip und Transparenz 9
3.1 Auszug aus Nr. 3 der Richtlinie 9
3.2 Durchführungsbestimmungen 9
4 Personal 10
4.1 Auszug aus Nr. 4 der Richtlinie 10
4.2 Durchführungsbestimmungen 10
5 Ansprechperson für Korruptionsprävention 14
5.1 Auszug aus Nr. 5 der Richtlinie 14
5.2 Durchführungsbestimmungen 15
6 Organisationseinheit zur Korruptionsprävention 17
6.1 Auszug aus Nr. 6 der Richtlinie 17
6.2 Durchführungsbestimmungen 17
7 Sensibilisierung und Belehrung der Beschäftigten 18
7.1 Auszug aus Nr. 7 der Richtlinie 18
7.2 Durchführungsbestimmungen 18
8 Aus- und Fortbildung 22
8.1 Auszug aus Nr. 8 der Richtlinie 22
8.2 Durchführungsbestimmungen 22
9 Konsequente Dienst- und Fachaufsicht 24
9.1 Auszug aus Nr. 9 der Richtlinie 24
9.2 Durchführungsbestimmungen 24
10 Unterrichtung und Maßnahmen bei Korruptionsverdacht 26
10.1 Auszug aus Nr. 10 der Richtlinie 26
10.2 Durchführungsbestimmungen 26
11 Leitsätze für die Vergabe 28

11.1 Auszug aus Nr. 11der Richtlinie 28
11.2 Durchführungsbestimmungen 28

12 Antikorruptionsklausel, Verpflichtungsgesetz 30
12.1 Auszug aus Nr. 12 der Richtlinie 30
12.2 Durchführungsbestimmungen 30

13 Zuwendungen an Dienststellen, Sponsoring 31
13.1 Auszug aus Nr. 13 der Richtlinie 31
13.2 Durchführungsbestimmungen 31

14 Zuwendungsempfänger 32
14.1 Auszug aus Nr. 14 der Richtlinie 32
14.2 Durchführungsbestimmungen 32

Zweck

Diese Zentrale Dienstvorschrift beinhaltet Regelungen zur Konkretisierung und weiteren Ausgestaltung der *„Richtlinie der Bundesregierung zur Korruptionsprävention in der Bundesverwaltung“*[1] (Richtlinie). Sie trägt insbesondere den organisatorischen und fachlichen Besonderheiten im Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg) Rechnung und gibt einen einheitlichen Handlungsrahmen bei der Umsetzung der Korruptionsprävention in der Bundeswehr vor. Darüber hinaus legt sie fest, in welcher Weise die vom Bundesministerium des Innern (BMI) herausgegebenen *„Empfehlungen zur Korruptionsprävention in der Bundesverwaltung“*[2] (Empfehlungen) Anwendung finden.

In der Richtlinie werden zur Vermeidung und Eindämmung von Korruptionstaten die wesentlichen Elemente der für den Bund maßgeblichen Strategie vorgegeben. Ihre Beachtung ist dauerhafter Auftrag und Verpflichtung für alle in den Geltungsbereich dieser Regelung einbezogenen Dienststellen und Gesellschaften der Bundeswehr.

Für den Begriff der Korruption gibt es keine gesetzliche Definition. Mit einer Korruptionshandlung ist der Missbrauch eines öffentlichen Amtes, einer Funktion in der Wirtschaft oder eines politischen Mandats verbunden. Hierbei erfolgt die Beeinflussung eines Entscheidungsträgers durch die Gewährung unzulässiger Vorteile. Ziel des Vorteilgebers ist die sachwidrige Vornahme oder das Unterlassen einer bestimmten Handlung zu seinen Gunsten oder zu Gunsten von Dritten.

Durch Korruption können erhebliche materielle und immaterielle Schäden (z. B. Personenschäden durch die Nutzung fehlerhafter Ausrüstung) entstehen, die sich negativ auf die Funktionsfähigkeit der öffentlichen Verwaltung auswirken und das Vertrauen der Allgemeinheit in deren Integrität und Funktionsfähigkeit nachhaltig beeinträchtigen.

[1] VMBl 2006 S. 19
[2] BMI - Az O4 - 013 001 - 1/3 vom 9. Februar 2012; im Intranet Bw bereitgestellt unter: http://intranet.bmvg/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzIyZTMyMzUzMTMwMzAzMDMwMzAzMDY4Njk3YTczNjQ3MDZiNjMyMDIwMjAyMDIw/120209%20final%20Empfehlungen.pdf

1 Anwendungsbereich

1.1 Auszug aus Nr. 1 der Richtlinie

1 Anwendungsbereich

1.1 Die Maßnahmen aller Dienststellen des Bundes zur Korruptionsprävention bestimmen sich nach dieser Richtlinie; als Dienststellen des Bundes gelten die obersten Bundesbehörden, die Behörden der unmittelbaren und mittelbaren Bundesverwaltung, die Gerichte des Bundes und Sondervermögen des Bundes. Die Vorschrift findet auch auf die Streitkräfte Anwendung; Einzelheiten regelt das Bundesministerium der Verteidigung.

1.2 Diese Richtlinie gilt sinngemäß auch für juristische Personen des öffentlichen oder privaten Rechts, an denen ausschließlich die Bundesrepublik Deutschland beteiligt ist.

1.3 Im Übrigen ist den jeweiligen organisatorischen und fachlichen Besonderheiten Rechnung zu tragen.

1.2 Durchführungsbestimmungen

101. Die Richtlinie findet im BMVg, in der Bundeswehrverwaltung, der Rechtspflege der Bundeswehr (mit Ausnahme der Spruchkörper in den Truppendienstgerichten), der Militärseelsorge und in den Streitkräften unmittelbar Anwendung. Sie ist deshalb von den betreffenden Dienststellenleitungen nach Maßgabe dieser Durchführungsbestimmungen sowie sonstiger Weisungen umzusetzen.

102. Unter einer sinngemäßen Anwendung im Sinne von Nr. 1.2 der Richtlinie ist zu verstehen, dass sie von den dort aufgeführten juristischen Personen des öffentlichen Rechts (Körperschaften, Anstalten, Stiftungen) und des privaten Rechts (rechtsfähige Vereine, Stiftungen, Kapitalgesellschaften) anzuwenden ist, soweit die betreffende Rechtsform dem nicht entgegen steht.

Ist die Bundesrepublik Deutschland nicht alleiniger Anteilseigner einer Gesellschaft mit vom BMVg geführter Bundesbeteiligung, so wirkt die Beteiligungsführung im Rahmen der ihr nach Rechtsform und Beteiligungsverhältnissen zustehenden Einflussmöglichkeiten auf eine sinngemäße Anwendung der Richtlinie oder auf sonstige geeignete Maßnahmen zur Korruptionsprävention hin.

103. Sofern eine sinngemäße Anwendung der Richtlinie nicht in Betracht kommt, kann die Erstellung von internen Richtlinien ein wichtiges und effektives Hilfsmittel sein, um sensible Bereiche zu regeln und für die Beschäftigten der juristischen Person Handlungssicherheit in Bezug auf zulässiges Verhalten zu schaffen. Hierbei wird empfohlen, insbesondere folgende Handlungsfelder der Korruptionsprävention zu regeln:

- Ausrichtung der Geschäftspraktiken an ethischen Werten,
- Identifizierung besonders korruptionsgefährdeter Arbeitsbereiche und Analyse bestehender Sicherungsmaßnahmen,
- in Abhängigkeit von der Größe einer Institution Einrichtung einer Ansprechstelle für Fragen der Korruptionsprävention/eines Compliance Office (einschließlich Verfahren für Hinweisgeber/ innen),
- interne Kontrollen,
- Verhalten gegenüber Geschäftspartnern und Amtspersonen in Bezug auf die Entgegennahme und Verteilung von Zuwendungen gleich welcher Art und welchen Wertes,
- Verhalten bei Interessenkollisionen,
- Aufnahme und Ausübung von Nebentätigkeiten,
- Sensibilisierung und Fortbildung der Beschäftigten auf dem Gebiet der Korruptionsprävention (Darstellung der strafrechtlichen Situation mit Bezug auf die Delikte im Bereich der Korruption) und
- Anwendung von Antikorruptionsklauseln.

104. Die Richtlinie gilt unter Berücksichtigung einsatzbedingter Gegebenheiten auch bei Einsätzen der Bundeswehr außerhalb der Bundesrepublik Deutschland. Einzelheiten für die Einsatzdienststellen regeln das Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr (BAIUDBw) und das Einsatzführungskommando der Bundeswehr (EinsFüKdoBw) in gesonderten Weisungen. Ein gegenseitiger Informationsaustausch ist sicherzustellen.

2 Besonders korruptionsgefährdete Arbeitsgebiete

2.1 Auszug aus Nr. 2 der Richtlinie

2 Feststellen und Analysieren besonders korruptionsgefährdeter Arbeitsgebiete

In allen Dienststellen des Bundes sind in regelmäßigen Abständen sowie aus gegebenem Anlass die besonders korruptionsgefährdeten Arbeitsgebiete festzustellen.

Für diese ist die Durchführung von Risikoanalysen zu prüfen. Je nach den Ergebnissen der Risikoanalyse ist zu prüfen, wie die Aufbau-, Ablauforganisation und/oder die Personalzuordnung zu ändern sind.

2.2 Durchführungsbestimmungen

201. Bei der Feststellung besonders korruptionsgefährdeter Arbeitsgebiete handelt es sich um die zentrale Präventionsmaßnahme nach der Richtlinie. Hierzu ist eine Bewertung vorzunehmen, welche möglichen Korruptionsgefahren im Zusammenhang mit den einem Dienstposten zugeordneten Aufgaben bestehen (Gefährdungsanalyse). Im Rahmen dieser (von der Richtlinie vorgesehenen) Prüfung sind die Arbeitsgebiete einzelfallbezogen zu betrachten. Alle mit einem dienstlichen Arbeitsgebiet verbundenen Aufgaben bzw. Funktionen und damit einhergehenden Kontakte, Arbeitsbeziehungen, Handlungs-, Weisungs- sowie Entscheidungsmöglichkeiten sind deshalb in die Untersuchungen einzubeziehen. Hierbei ist allgemein zu berücksichtigen, dass Faktoren, die zu einer Konzentration von Verantwortlichkeiten bzw. einer Reduzierung von Bewertungsinstanzen führen, eine Erhöhung des Korruptionsrisikos nach sich ziehen können.

Das Verfahren und der Beurteilungsmaßstab bei der Feststellung besonders korruptions-gefährdeter Arbeitsgebiete richten sich nach den vom Bundesministerium des Innern (BMI) herausgegebenen Empfehlungen. Als Hilfestellung zur Planung und Durchführung der einzelnen Verfahrensschritte kann die dort genannte *„Handreichung der AG Standardisierung zur Feststellung besonders korruptionsgefährdeter Arbeitsgebiete“*[3] verwendet werden. Die Ergeb- nisse der Gefährdungs- und einer sich ggf. anschließenden Risikoanalyse sowie die hierauf aufsetzenden Maßnahmen sind von den untersuchenden Stellen zusammenzustellen und nachvollziehbar zu dokumentieren.

[3] BMI – Az O4 - 013 001 – 1/6 vom 4. Januar 2012; im IntranetBw bereitgestellt unter: http://intranet.bmvg/portal/a/i_bmvg/!ut/p/c4/HYpBDoAgDMDe4gfY3Zu_UC9mkIELMMhQ_L5Kemmawg4fqp0DXlwEE6ywOZ7tY_iwuQfj0Z0svmgeh4lF9a6_tqpInWRkTCIQJhZqUOMyvW2FG94!/

202. Prüfungen zur Feststellung besonders korruptionsgefährdeter Arbeitsgebiete sind spätestens nach einem Zeitraum von fünf Jahren nach Abschluss einer vorhergehenden Untersuchung zu wiederholen. Wenn organisatorische Entscheidungen eine vollständige oder weitgehende Veränderung des Aufbaus eines Organisationselementes bzw. der ihm zugeordneten Aufgaben nach sich ziehen, sind anlassbezogene Untersuchungen zum frühestmöglichen Zeitpunkt durchzuführen. Gleiches gilt für einzelne Arbeitsgebiete (Dienstposten), wenn Erkenntnisse vorliegen, die eine Überprüfung der bisherigen Einstufung rechtfertigen. Sollen regelmäßige oder anlassbezogene Feststellungen im Sinne vorstehender Sätze 1 bis 3 ausnahmsweise zu einem späteren Zeitpunkt stattfinden, ist die vorherige Zustimmung von BMVg – R II 1 unter Darlegung der Gründe einzuholen.

B

203. Im Hinblick auf die Prüfung und Durchführung von Risikoanalysen in besonders korruptionsgefährdeten Arbeitsgebieten ist nach Nr. 3 der Empfehlungen zu Nr. 2 der Richtlinie zu verfahren. Zur Untersuchung und Bewertung des Korruptionsrisikos sowie der Wirksamkeit bestehender Sicherungsmaßnahmen kann auf Anlage 5 der vom BMI herausgegebenen „*Handreichung der AG Standardisierung zur Feststellung besonders korruptionsgefährdeter Arbeitsgebiete“* zurückgegriffen werden.

204. **Besonders** korruptionsgefährdete Arbeitsgebiete sind für zielgerichtete Steuerungsmaßnahmen zur Korruptionsprävention zwingend in den Organisationsgrundlagen auszuweisen und stehen damit auch dem Personalwirtschaftssystem der Bundeswehr zur Verfügung. Zur entsprechenden Kennzeichnung von Dienstposten verfügt die den Hauptprozess Organisation unterstützende Software SAP über ein Merkmalfeld „Korruptionsgefährdung“[4]. Sofern ein besonders korruptionsgefährdetes Arbeitsgebiet nicht mit einem Dienstposten hinterlegt ist und die betroffenen Aufgaben stattdessen einem eingerichteten „Dienstpostenähnlichen Konstrukt“ (DPäK) zuzuordnen sind, ist die zuständige personalbearbeitende Stelle über die Feststellung der besonderen Korruptionsgefährdung zu unterrichten. Sinngemäß ist bei Langzeit-/ Dauerkommandierungen im Rahmen von (temporären) Projektgruppen zu verfahren. Nr. 201 Satz 8 bleibt unberührt.

[4] Sofern die Feststellungen nach Nr. 201 bei einzelnen Arbeitsgebieten zu dem Ergebnis führen, dass für diese lediglich die im ersten Verfahrensschritt zu prüfenden Voraussetzungen für ein „korruptions- gefährdetes Arbeitsgebiet“ vorliegen (Nr. 1.2 der Empfehlungen zu Nr. 2 der Richtlinie), kann die untersuchende Stelle auch dieses Resultat durch Nutzung des Merkmalfeldes „Korruptionsgefährdung“ in die Software SAP einpflegen. Die Pflicht zur nachvollziehbaren Zusammenstellung und Dokumentation der Feststellungen gemäß Nr. 201 Satz 8 bleibt jedoch unberührt.

3 Mehr-Augen-Prinzip und Transparenz

3.1 Auszug aus Nr. 3 der Richtlinie

3 Mehr-Augen-Prinzip und Transparenz

3.1 Vor allem in besonders korruptionsgefährdeten Arbeitsgebieten ist das Mehr-Augen-Prinzip (Beteiligung bzw. Mitprüfung durch mehrere Beschäftigte oder Organisationseinheiten) sicherzustellen. Stehen dem Rechtsvorschriften oder unüberwindliche praktische Schwierigkeiten entgegen, kann die Mitprüfung auf Stichproben beschränkt werden oder es sind zum Ausgleich andere Maßnahmen der Korruptionsprävention (z. B. eine intensivere Dienst- und Fachaufsicht) vorzusehen.

3.2 Die Transparenz der Entscheidungen einschließlich der Entscheidungsvorbereitung ist sicherzustellen (z. B. durch eindeutige Zuständigkeitsregelung, Berichtswesen, IT-gestützte Vorgangskontrolle, genaue und vollständige verfahrensbegleitende Dokumentation).

3.2 Durchführungsbestimmungen

301. Aufbau- und ablauforganisatorische Maßnahmen sind so zu treffen, dass in Bereichen mit einem erhöhten Risiko von Korruption die Gefahr korruptiver Handlungen minimiert wird. Dabei ist die Beachtung des Mehr-Augen-Prinzips von besonderer Bedeutung. Dessen Ziel ist es, Entscheidungen und Tätigkeiten einer mehrfachen Kontrolle zu unterziehen (Ausweitung der Kontrolle) oder mehrere (unabhängige, unvoreingenommene) Personen an der Absicherung einer Entscheidung oder Tätigkeit zu beteiligen (Aufteilung von Entscheidungskompetenzen).

Werden im Rahmen der Gefährdungsanalyse besonders korruptionsgefährdete Arbeitsgebiete festgestellt (Nr. 2 Satz 1 der Richtlinie), ist bei den anschließenden Prüfungen bzw. den Risikoanalysen stets zu untersuchen, ob das Mehr-Augen-Prinzip ausreichend Berücksichtigung findet. Sofern eine Anwendung des Mehr-Augen-Prinzips ausnahmsweise nicht möglich sein sollte, ist zu prüfen, welche anderweitig geeigneten und wirksamen Maßnahmen zur Korruptionsprävention ergriffen werden können. Dienst- bzw. Arbeitsanweisungen oder sonstige Vorschriften zur Gestaltung der Arbeitsabläufe sind ggf. anzupassen.

302. Im Übrigen finden die Empfehlungen zu Nr. 3 der Richtlinie Anwendung.

4 Personal

4.1 Auszug aus Nr. 4 der Richtlinie

4 Personal

4.1 Das Personal für besonders korruptionsgefährdete Arbeitsgebiete ist mit besonderer Sorgfalt auszuwählen.

4.2 In besonders korruptionsgefährdeten Bereichen ist die Verwendungsdauer des Personals grundsätzlich zu begrenzen; sie sollte in der Regel eine Dauer von fünf Jahren nicht überschreiten. Bei einer erforderlichen Verlängerung sind die Gründe aktenkundig zu machen.

4.2 Durchführungsbestimmungen

401. Führt die Verwendung auf einem bestimmten Dienstposten zu einer Tätigkeit in einem besonders korruptionsgefährdeten Arbeitsgebiet, so sind die für eine Besetzung in Betracht kommenden Betroffenen hinsichtlich der in ihrer Person begründet liegenden Risiken zu überprüfen. Indikatoren hierfür könnten arbeitsrechtliche Maßnahmen, laufende strafrechtliche und disziplinare (Vor-)Ermittlungsverfahren, gerichtliche Disziplinar- oder Strafverfahren sowie bereits rechtskräftige Verurteilungen sein. Nr. 1 der Empfehlungen zu Nr. 4 der Richtlinie ist bei der Personalauswahl zu beachten.

Die für eine Verwendung in einem besonders korruptionsgefährdeten Arbeitsgebiet in Betracht kommenden Personen sind bereits im Personalauswahlverfahren (z. B. Vorstellungsgespräch/ Personalgespräch) auf die besondere Korruptionsgefährdung des Arbeitsgebietes hinzuweisen. Sie sind auch darüber zu informieren, dass an eine Verwendung auf diesem Dienstposten spezifische Maßnahmen der Korruptionsprävention (insbesondere eine grundsätzlich vorgesehene Begrenzung der Verwendungsdauer) geknüpft sind. Wird einem Dienstposten zu einem späteren Zeitpunkt ein besonders korruptionsgefährdetes Arbeitsgebiet zugeordnet oder erfolgt eine solche Feststellung anlässlich entsprechender Untersuchungen nach Nr. 2 der Richtlinie, ist die Dienstposteninhaberin/der Dienstposteninhaber durch die personalbearbeitende Stelle hierüber unverzüglich zu informieren und über die damit verbundenen besonderen Maßnahmen der Korruptionsprävention, d. h. bis hin zur Personalrotation, in Kenntnis zu setzen.

402. Es ist ständige Aufgabe der Dienst- und Fachaufsicht, einer unerwünschten Verfestigung von personellen Strukturen im Verkehr mit der Wirtschaft vorzubeugen und insoweit der Gefahr der Entstehung korruptiver Beziehungsgeflechte zu begegnen; dies gilt insbesondere in Bereichen mit identischen industriellen Ansprechpartnern. Rotationen können als zweckmäßiges Instrument genutzt werden, um der Entstehung eines korruptionsfördernden Näheverhältnisses vorzubeugen. Unabhängig davon, ob eine Verwendung in einem besonders korruptionsgefährdeten Arbeitsgebiet erfolgt, können deshalb von der Beschäftigungsstelle im Bedarfsfall mit der personalbearbeitenden Stelle Notwendigkeit und Möglichkeiten von Rotationsmaßnahmen geprüft werden, um der Korruption vorzubeugen.

403. Dem Rotationsgebot nach Nr. 4.2 der Richtlinie kann sowohl durch einen Verwendungswechsel der betroffenen Beschäftigten (Personalrotation) als auch durch den Wechsel der besonders korruptionsgefährdeten Aufgabe zu einem anderen Dienstposten (Aufgabenrotation) entsprochen werden. Es obliegt den personalbearbeitenden Stellen, die Verweildauer der Betroffenen auf Dienstposten mit besonders korruptionsgefährdeten Arbeitsgebieten zu erfassen und zu überwachen.

404. Rotationsmaßnahmen sollen mit zureichendem zeitlichen Vorlauf geplant werden, um die Funktionsfähigkeit der betroffenen Arbeitseinheiten nicht nachteilig zu beeinträchtigen und den Beschäftigten perspektivisch Möglichkeiten für eine weitere Verwendung eröffnen zu können. Zur Personalrotation sind hierzu geeignete Vorgaben, z. B. im Rahmen der Personalentwicklung, möglichst zu nutzen. Gleiches gilt für die Umsetzung von Maßnahmen zur Aufgabenrotation.

405. Die Verwendungsdauer von Personal in besonders korruptionsgefährdeten Arbeitsgebieten soll in der Regel eine Dauer von fünf Jahren nicht überschreiten. Beginn der Verwendungsdauer ist dabei der Zeitpunkt, der für die erstmalige Aufnahme der Tätigkeit in einem besonders korruptionsgefährdeten Arbeitsgebiet bestimmt wird.

Die personalbearbeitende Stelle zeigt der Beschäftigungsstelle rechtzeitig – spätestens jedoch nach einer Verweildauer von vier Jahren und sechs Monaten – erstmals an, dass aus Gründen der Korruptionsprävention ein Verwendungswechsel der Dienstposteninhaberin/des Dienstpostenin- habers anzustreben ist. Personalbearbeitende Stelle und Beschäftigungsstelle prüfen anschließend gemeinsam die Möglichkeit von Personalmaßnahmen. Sollte eine Personalmaßnahme aus fachlichen Gründen oder aus Personalführungsgründen nicht möglich sein, beurteilt die Beschäftigungsstelle unter Einbindung der für Organisationsfragen zuständigen Stelle zusätzlich die Option der Verlagerung besonders korruptionsgefährdeter Aufgaben. Die für Organisation zuständige Stelle entscheidet abschließend über die Möglichkeit einer Aufgaben- rotation. Die personalbearbeitende Stelle ist gegebenenfalls zur Berücksichtigung soldaten-, beamten- oder tarifrechtlicher Auswirkungen zu beteiligen. Über das Ergebnis der Prüfung einer möglichen Aufgabenrotation ist sie durch die Beschäftigungsstelle zu unterrichten.

406. Soweit aufgrund von gesetzlichen bzw. tarifvertraglichen Regelungen oder aufgrund von bereits konkret geplanten Personalführungsmaßnahmen gesichert ist, dass die Dienstposten-inhaberin/der Dienstposteninhaber bei Ablauf der fünfjährigen Frist nach Nr. 404 Satz 1 innerhalb der nächsten zwölf Monate ihre/seine Tätigkeit im bisherigen besonders korruptionsgefährdeten Arbeitsgebiet endgültig beenden oder **durchgängig für mindestens zwei Jahre** unterbrechen wird (z. B. Beendigung des Dienst- oder Arbeitsverhältnisses, Beurlaubung, Elternzeit, Umsetzung, Versetzung), kann eine Prüfung von Rotationsmaßnahmen im Einzelfall unterbleiben. Es ist jedoch unzulässig, das Rotationsgebot auf der Basis unspezifischer und unzureichend konkretisierter Planungsannahmen oder -fiktionen zu umgehen.

Einer Rotation können ferner Sachverhalte entgegenstehen, bei denen – insbesondere aus zwingenden Personalführungsgründen – das dienstliche Interesse an einem Verbleib im besonders korruptionsgefährdeten Arbeitsgebiet gegenüber den Belangen der Korruptions- prävention überwiegt. Im Rahmen der insoweit notwendigen Abwägung könnten beispielsweise folgende Umstände zum Verzicht auf eine Rotation führen, wobei jeder Einzelfall sorgfältig zu prüfen ist:

- Besondere berufliche Qualifikationen der Dienstposteninhaberin/des Dienstposteninhabers, ggf. einhergehend mit einem hohen Maß an hierauf beruhender Spezialisierung (keine reine Erfahrungsspezialisierung durch eine langjährige Verwendung),
- Wahrnehmung von herausgehobenen Leitungsaufgaben oder Ämtern, für die die fortdauernde Übereinstimmung mit den grundsätzlichen politischen Ansichten und Zielen der Bundesregierung erforderlich ist (ab Besoldungsgruppe B 6) sowie
- Spezielle rechtliche Vorgaben (z. B. Sicherheitsüberprüfungsgesetz, Sozialgesetzbuch IX).

In allen Fällen, in denen eine Verlängerung der Verwendungsdauer über die Frist von fünf Jahren hinaus erforderlich ist, sind die hierfür maßgeblichen Gründe durch die personalbearbeitende Stelle aktenkundig zu machen (Nr. 4.2 der Richtlinie). Anschließend sind von der Beschäfti- gungsstelle geeignete und wirksame **Ausgleichsmaßnahmen** zur Verminderung des Korruptions- risikos zu treffen und ebenfalls aktenkundig zu machen. Dies können z. B. sein:

- Erweiterung des Mehr-Augen-Prinzips (Ausweitung der Kontrolle; Aufteilung von Entscheidungskompetenzen; Regelungen zur Mitzeichnung, die fachnahe Zweitprüfung vorsehen),
- Änderung der Aufbau- und Ablauforganisation (z. B. Verlagerung von Zuständigkeiten [Wahrnehmung von Außenkontakten durch mehrere Bedienstete, Einführung von Teamarbeit]),
- Verstärkung der Fach- und Dienstaufsicht (z. B. vermehrte stichprobenartige Überprüfung von Vorgängen unter dem Blickwinkel der Korruptionsprävention) sowie
- Regelmäßige und anlassbezogene Sensibilisierungen.

Die personalbearbeitende Stelle ist dabei gegebenenfalls zur Berücksichtigung soldaten-, beamten- oder tarifrechtlicher Auswirkungen zu beteiligen.

407. Unbeschadet des Absehens von Rotationsmaßnahmen ist grundsätzlich auf die Beseitigung vorliegender Hinderungsgründe für eine Rotation hinzuwirken. Die personal- bearbeitende Stelle entscheidet in Abhängigkeit von den konkret vorliegenden Hinderungsgründen für eine Rotation, wann sie mit dem Ziel eines Verwendungswechsels erneut auf die Beschäfti- gungsstelle zugeht. Wurde von der Durchführung einer Rotation abgesehen und entfallen die hierfür ausschlaggebenden Gründe nachträglich, ist erneut ein Verwendungs- oder Aufgaben- wechsel zu prüfen.

408. Bei Auswahl und Gestaltung der Ausgleichsmaßnahmen und bei der Planung von Aufgabenrotationen ist die Ansprechperson für Korruptionsprävention kontinuierlich zu beteiligen. Sie berät die verantwortlichen Entscheidungsträger und unterstützt diese im Rahmen ihrer fachlichen Expertise bei der Entwicklung praxisgerechter Lösungsansätze zur Verminderung des Korruptionsrisikos. Ein Anspruch auf Beteiligung an Personalmaßnahmen besteht nicht.

5 Ansprechperson für Korruptionsprävention

5.1 Auszug aus Nr. 5 der Richtlinie

5 Ansprechperson für Korruptionsprävention

5.1 *Abhängig von Aufgabe und Größe der Dienststelle ist eine Ansprechperson für Korruptionsprävention zu bestellen. Sie kann auch für mehrere Dienststellen zuständig sein. Ihr können folgende Aufgaben übertragen werden:*

a) Ansprechpartner bzw. Ansprechpartnerin für Beschäftigte und Dienststellenleitung, auch ohne Einhaltung des Dienstweges, sowie für Bürgerinnen und Bürger;
b) Beratung der Dienststellenleitung;
c) Aufklärung der Beschäftigten (z. B. durch regelmäßige Informationsveranstaltungen);
d) Mitwirkung bei der Fortbildung;
e) Beobachtung und Bewertung von Korruptionsanzeichen;
f) Mitwirkung bei der Unterrichtung der Öffentlichkeit über dienst- und strafrechtliche Sanktionen (Präventionsaspekt) unter Beachtung der Persönlichkeitsrechte der Betroffenen.

5.2 *Werden der Ansprechperson Tatsachen bekannt, die den Verdacht einer Korruptionsstraftat begründen, unterrichtet sie die Dienststellenleitung und macht in diesem Zusammenhang Vorschläge zu internen Ermittlungen, zu Maßnahmen gegen Verschleierung und zur Mitteilung an die Strafverfolgungsbehörden. Die Dienststellenleitung veranlasst die zur Aufklärung des Sachverhalts erforderlichen Schritte.*

5.3 *Der Ansprechperson dürfen keine Disziplinarbefugnisse übertragen werden; in Disziplinarverfahren wegen Korruption wird sie nicht als Ermittlungsführer tätig.*

5.4 *Die Dienststellen haben die Ansprechperson zur Wahrnehmung ihrer Aufgaben rechtzeitig und umfassend zu informieren, insbesondere bei korruptionsverdächtigen Vorfällen.*

5.5 *Bei der Wahrnehmung ihrer Aufgaben zur Korruptionsprävention ist die Ansprechperson weisungsunabhängig. Sie hat ein unmittelbares Vortragsrecht bei der Dienststellenleitung und darf wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden.*

5.6 *Die Ansprechperson hat über ihr bekannt gewordene persönliche Verhältnisse von Beschäftigten, auch nach Beendigung ihrer Amtszeit, Stillschweigen zu bewahren; dies gilt nicht gegenüber der Dienststellenleitung und der Personalverwaltung, wenn sie Tatsachen erfährt, die den Verdacht einer Korruptionsstraftat begründen. Personenbezogene Daten sind nach den Grundsätzen der Personalaktenführung zu behandeln.*

5.2 Durchführungsbestimmungen

501. Über die Frage der Bestellung einer Ansprechperson für Korruptionsprävention und einer Stellvertretung entscheidet die Dienststellenleitung nach pflichtgemäßem Ermessen (Nr. 5.1 der Richtlinie), soweit und solange diesbezüglich keine Weisungen vorgesetzter Dienststellen ergangen sind[5]. Die Bestellung erfolgt schriftlich durch die Dienststellenleitung und ist mit einer konkreten Aufgabenübertragung für diese Funktion zu verbinden. Die Beschäftigten der betreuten Dienststelle(n) sind in geeigneter Weise (z. B. Aushang, Stabsbefehl, Intranetpräsenz) über die Erreichbarkeit und die Aufgaben der für sie zuständigen Ansprechperson sowie der Ansprechperson der vorgesetzten Dienststelle und des BMVg[6] in Kenntnis zu setzen.

502. Neben den in Nr. 5.1 der Richtlinie genannten Aufgaben kann die Ansprechperson die mit der Umsetzung der Korruptionsprävention beauftragten Organisationselemente oder Stellen fachlich beraten und begleitend unterstützen. In diesen Fällen sind ihr das hierfür relevante Aktenmaterial sowie sonstige Aufzeichnungen und Informationen zur Verfügung zu stellen.

503. Werden der Ansprechperson Tatsachen bekannt, die den Verdacht einer Korruptions- straftat begründen, ist die Dienststellenleitung zu unterrichten und im Übrigen nach den Durchführungsbestimmungen zu Nr. 10 der Richtlinie zu verfahren. Allgemeine Empfehlungen und Hilfestellungen zum konkreten Umgang der Ansprechperson für Korruptionsprävention mit Korruptionsverdachtsfällen und Hinweisgebern enthält ferner die vom BMI herausgegebene „*Handreichung für die Arbeitsweise der Ansprechperson für Korruptionsprävention bei Verdachtsfällen*“[7].

504. Als Ansprechperson für Korruptionsprävention dürfen im Geschäftsbereich des BMVg nicht bestellt werden:

- Sicherheitsbeauftragte (ZDv 2/30, Nrn. 111, 114, zukünftig: ZDv A-1130/1) sowie Beschäftigte, die mit Sicherheitsüberprüfungen befasst sind. Die Nutzung und Übermittlung personenbezogener Daten aus Sicherheitsüberprüfungen unterliegt einer strengen gesetzlichen Zweckbindung (§§ 21, 37 Sicherheitsüberprüfungsgesetz – SÜG), die eine Weitergabe solcher Einzeldaten **an die Ansprechperson für Korruptionsprävention –** sowohl bei Vorliegen eines Korruptionsverdachts, als auch für allgemeine Belange der Korruptionsprävention – nicht zulässt;
- Dienststellenleitungen und Beschäftigte mit Disziplinarbefugnissen;
- Personen, die als Vertreter des Bundeswehrdisziplinaranwalts, einer Wehrdisziplinaranwaltschaft oder im Auftrag eines Dienstvorgesetzten in Disziplinarverfahren tätig sind.

[5] z. B. Weisungen zur Korruptionsprävention in einzelnen Organisationsbereichen der Bundeswehr oder Festlegungen von militärischen Kommandobehörden über die Zuständigkeit der Ansprechperson einer Dienststelle auch für weitere Dienststellen oder dislozierte Teile von Dienststellen.
[6] Bundesministerium der Verteidigung, R II 1, Postfach 13 28, 53003 Bonn
[7] BMI – Az O4-15002/12 vom 20. September 2013; im IntranetBw bereitgestellt unter http://intranet.bmvg/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzIyZTMyMzUzMTMwMzAzMDMwMzAzMDY4NmM3OTc1NjI3NzYzNzUyMDIwMjAyMDIw/Handreichung%20Ansprechperson.pdf

Beschäftigte, die Dienst- und/oder Fachaufsicht über Maßnahmen der Korruptionsprävention ausüben, sollen nicht als Ansprechperson für Korruptionsprävention bestellt werden, wenn die mit der Tätigkeit als Ansprechperson im Zusammenhang stehenden Aufgaben zugleich Gegenstand der Beaufsichtigung sind (Vermeidung von Interessenkonflikten bzw. der Gefahr einer Selbstkontrolle).

6 Organisationseinheit zur Korruptionsprävention

6.1 Auszug aus Nr. 6 der Richtlinie

6 Organisationseinheit zur Korruptionsprävention

Wenn Ergebnisse von Risikoanalysen oder besondere Anlässe es erfordern, sollte befristet oder auf Dauer eine gesonderte weisungsunabhängige Organisationseinheit zur Überprüfung und Bündelung der im jeweiligen Hause praktizierten Maßnahmen zur Korruptionsprävention eingerichtet werden; es besteht ein unmittelbares Vortragsrecht bei der Dienststellenleitung. Diese Aufgabe kann auch von der Innenrevision wahrgenommen werden. Bei Mängeln in der Korruptionsprävention unterrichtet diese Organisationseinheit die Dienststellenleitung und die Ansprechperson für Korruptionsprävention unmittelbar; sie soll Empfehlungen für geeignete Änderungen unterbreiten.

6.2 Durchführungsbestimmungen

601. Wegen des besonderen Stellenwertes der Korruptionsprävention ist im BMVg mit dem Referat R II 1 auf Dauer eine Organisationseinheit für diese Aufgabe eingerichtet.

BMVg – R II 1 nimmt auf ministerieller Ebene die Grundsatzaufgaben auf dem Gebiet der Korruptionsprävention wahr und legt durch zentrale Vorgaben den Handlungsrahmen zur Ausgestaltung der Präventionsmaßnahmen sowie für eine einheitliche Umsetzung der Richtlinie in den Organisationsbereichen der Bundeswehr fest. Darüber hinaus koordiniert BMVg – R II 1 bei Grundsatzfragen die Belange der Korruptionsprävention an den Schnittstellen zu anderen Fachaufgaben, nimmt konzeptionelle und Bedarfsträgeraufgaben für zentrale Qualifizierungsmaßnahmen wahr, wirkt an der Weiterentwicklung der Präventionsarbeit mit und vertritt im eigenen Aufgabenbereich die Interessen des Bundesministeriums der Verteidigung im Dialog mit Dritten.

Für die Wahrnehmung der Dienst- und Fachaufsicht gelten die Durchführungsbestimmungen zu Nr. 9 der Richtlinie.

Die Aufgaben der Referate Revision im BMVg und Revision Bw (Referat ZA I 5) im BAIUDBw bleiben unberührt.

602. Soweit die Aufgaben für Korruptionsprävention innerhalb einer Dienststelle auf unterschiedliche Organisationselemente verteilt sind, stellen die Dienststellenleitungen durch ablauforganisatorische Regelungen sicher, dass die jeweiligen Zuständigkeiten dokumentiert werden und der Informationsfluss sowie die gegenseitige Unterrichtung der beteiligten Stellen gewährleistet sind.

7 Sensibilisierung und Belehrung der Beschäftigten

7.1 Auszug aus Nr. 7 der Richtlinie

7 Sensibilisierung und Belehrung der Beschäftigten

7.1 Die Beschäftigten sind anlässlich des Diensteides oder der Verpflichtung auf Korruptionsgefahren aufmerksam zu machen und über die Folgen korrupten Verhaltens zu belehren. Die Belehrung ist zu dokumentieren. Hinsichtlich möglicher Korruptionsgefahren sind die Beschäftigten auch in der weiteren Folge zu sensibilisieren. Darüber hinaus soll ein „Verhaltenskodex gegen Korruption" (siehe Anlage 1) allen Beschäftigten vermitteln, was sie insbesondere in besonders korruptionsgefährdeten Arbeitsgebieten oder Situationen zu beachten haben.

7.2 Bei Tätigkeiten in besonders korruptionsgefährdeten Arbeitsgebieten – auch bei einem Wechsel dorthin – sollen in regelmäßigen Abständen eine erneute Sensibilisierung und eine vertiefte arbeitsplatzbezogene Belehrung der Beschäftigten erfolgen.

7.2 Durchführungsbestimmungen

701. Unter Sensibilisierung im Sinne von Nr. 7 der Richtlinie sind Aktivitäten zu verstehen, die auf die Begründung oder Vertiefung eines Problembewusstseins gerichtet sind und im Wege einer besonderen Ansprache die potenzielle Gefahr von Korruptionshandlungen vergegenwärtigen, Anleitung zu pflichtgemäßem Verhalten geben sowie Anlaufstellen in Zweifelsfragen benennen. Sensibilisierungsmaßnahmen erfolgen in aller Regel formlos.

Bei einer Belehrung im Sinne von Nr. 7 der Richtlinie handelt es sich demgegenüber um eine förmliche Aufklärung über den Regelungsgehalt von Rechtsvorschriften mit Bezug zur Korruptionsprävention und -bekämpfung. Dabei stehen insbesondere die in solchen Bestimmungen normierten Verhaltenspflichten und die bei Verstößen vorgesehenen Rechtsfolgen im Vordergrund.

702. Bei der Einstellung von Beamtinnen und Beamten bzw. von Arbeitnehmerinnen und Arbeitnehmern sind die entsprechenden Mitarbeiterinnen und Mitarbeiter anlässlich des Diensteides bzw. der Verpflichtung nach dem Verpflichtungsgesetz[8] aktenkundig über Korruptionsgefahren und die Folgen korrupten Verhaltens nach Nr. 7.1 der Richtlinie zu belehren (Erstbelehrung). Bei Soldatinnen und Soldaten ist die Erstbelehrung von der zuständigen personalbearbeitenden Stelle wie folgt vorzunehmen:

a) Bei Ableistung von Freiwilligem Wehrdienst als besonderes staatsbürgerliches Engagement (§ 58 b Soldatengesetz (SG)), nach Ablauf der sechsmonatigen Probezeit,

[8] BGBl. 1974 S. I 469, 547; geändert durch Gesetz vom 15. August 1974 (BGBl. I S. 1942)

b) Bei der Berufung in das Dienstverhältnis einer Soldatin bzw. eines Soldaten auf Zeit, soweit sie zu diesem Zeitpunkt noch nicht nach Buchstabe a) durchgeführt wurde,
c) Bei der Berufung in das Dienstverhältnisses einer Berufssoldatin bzw. eines Berufssoldaten, soweit sie zu diesem Zeitpunkt noch nicht nach Buchstabe a) oder b) durchgeführt wurde,
d) Bei der Heranziehung bzw. Aktivierung zu freiwilligen Dienstleistungen außerhalb des Spannungs- oder Verteidigungsfalls nach dem vierten Abschnitt des Soldatengesetzes, soweit sie zu diesem Zeitpunkt noch nicht anlässlich eines vorhergehenden Wehrdienstes nach den Buchstaben a) bis c) durchgeführt wurde,
e) Bei der Berufung in ein Reservewehrdienstverhältnis (§ 4 Reservistinnen- und Reservistengesetz (ResG)), soweit sie zu diesem Zeitpunkt noch nicht anlässlich eines vorhergehenden Wehrdienstes nach den Buchstaben a) bis d) durchgeführt wurde.

Abweichend hiervon sind Soldatinnen und Soldaten, deren Wehrdienstverhältnis wegen der Feststellung des Spannungs- oder Verteidigungsfalls nicht auf der Basis einer freiwilligen schriftlichen Verpflichtung begründet wurde, nur dann zu belehren, wenn sie in besonders korruptionsgefährdeten Arbeitsgebieten verwendet werden.

703. Zur Gewährleistung eines einheitlichen Standards ist für die Erstbelehrung das in der Formulardatenbank der Bundeswehr[9] elektronisch bereitgestellte Formblatt „Belehrung über mögliche Korruptionsgefahren und die Folgen korrupten Verhaltens“ (Bw-2611) zu verwenden. Für das Personal in Gesellschaften mit Bundesbeteiligung gemäß Nr. 1.2 der Richtlinie sind Erstbelehrungen unter Berücksichtigung der dort für die Beschäftigten geltenden Regularien inhaltlich zu gestalten.

704. Aufbauend auf die Belehrung zum Diensteinritt/zur Einstellung ist den Beschäftigten zur Erhaltung bzw. zum Ausbau der Wissensbasis von der Beschäftigungsstelle einmal jährlich eine Sammlung von Informationsunterlagen zur Kenntnis zu geben, um sie auch in der weiteren Folge für die Gefahren der Korruption zu sensibilisieren und vorhandene Kenntnisse aktuell zu halten. Die Sammlung soll folgende Bestandteile beinhalten:

- Verhaltenskodex gegen Korruption (Anlage 1 der Richtlinie),
- Erlass über die Annahme von Belohnungen und Geschenken in der jeweils gültigen Fassung[10],
- eine Sammlung von Beispielen realer Korruptionssachverhalte aus der Bundeswehr[11].

Ergänzend können bei Bedarf die Richtlinie sowie sonstige Unterlagen beigefügt werden, die den Besonderheiten einer Dienststelle oder sonstigen Einrichtung Rechnung tragen.

[9] http://zrp21.bundeswehr.org/fachinfo/i_terrwv/fi_i_terrwv_formulare.nsf/
[10] VMBl 2005 S. 126, Änderung VMBl 2007 S. 53.
[11] Im IntranetBw aufzurufen unter:
http://intranet.bmvg/portal/a/i_bmvg/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9zPik3LJ0vbTE5IzMvLT8olywCr3s_KKi0gIQs7igKDG1LDUPXThNvyDbUREARGWguw!!/

Der Leitfaden für Vorgesetzte (Anlage 2 der Richtlinie) ist dem in Frage kommenden Personen- kreis bereits bei Übernahme der Dienstgeschäfte auszuhändigen.

Für den Erfolg der Sensibilisierung ist insbesondere von Bedeutung, dass den Beschäftigten Notwendigkeit und Funktionsweise der Korruptionsprävention derart vermittelt werden, dass ein praktischer Bezug zum jeweiligen dienstlichen Aufgabenbereich hergestellt werden kann. Darüber hinaus sollte begleitend kommuniziert werden, dass Vorkehrungen zur Korruptionsprävention nicht Ausdruck mangelnden Vertrauens in die Integrität der Beschäftigten sind, sondern Schutz vor der Verwicklung in kriminelles Verhalten bieten. Neben der obligatorischen Sensibilisierung mittels schriftlicher Hinweise gemäß Satz 1 und 4 sind deshalb u. a. folgende Maßnahmen geeignet, eine auf Dauer angelegte Auseinandersetzung mit der Korruptionsprävention zu fördern:

- Vortrags- und Informationsveranstaltungen der Ansprechperson für Korruptionsprävention oder sonstiger Träger,
- Erörterung im Rahmen von Mitarbeitergesprächen[12], Dienstbesprechungen und anlässlich des sonstigen Gedankenaustauschs zwischen Vorgesetzten und Mitarbeiterinnen/Mitarbeitern bzw. Soldatinnen/Soldaten,
- Gestaltung einer gehaltvollen Intranetpräsenz,
- Informationsschreiben (Newsletter) zu relevanten Themen (z. B. Hinweise auf Publikationen, Rechtsprechung und Literatur) sowie
- Teilnahme an Qualifizierungsmaßnahmen. In diesem Zusammenhang besteht insbesondere auch die Möglichkeit zur Einschreibung in das für die Angehörigen der Bundesverwaltung entwickelte E-Learning-Programm[13] (vgl. auch Durchführungsbestimmungen zu Nr. 8 der Richtlinie).

[12] BMVg – Abteilungsleiter Personal – P I 1– Az 09-02-09 vom 4. Dezember 2013, Konzept für die Personalentwicklung in der Bundeswehr (KPersEntwBw), Nr. 5.1.1
[13] Im IntranetBw aufzurufen unter: https://lmsbw.ausbildung.bundeswehr.org/

705. Bei Aufnahme einer Tätigkeit in einem besonders korruptionsgefährdeten Arbeitsgebiet sind die betroffenen Beschäftigten von den Vorgesetzten im Hinblick auf das erhöhte Gefährdungspotenzial der neu übertragenen Aufgaben zu sensibilisieren und vertieft arbeitsplatzbezogen zu belehren. In diesem Zusammenhang sind die

- für das jeweilige Arbeitsgebiet konkret festgestellten Korruptionsrisiken,
- Zuständigkeiten bei der Aufgabenwahrnehmung,
- bestehenden Handlungs- und Gestaltungsbefugnisse und deren Grenzen,
- eingerichteten Kontrollen und Sicherungen,
- Maßnahmen bei erkannten Unregelmäßigkeiten im dienstlichen Umfeld sowie
- ggf. erwarteten Verhaltensgrundsätze als Vorgesetzter und Vorbild

vertrauensvoll mit den Dienstposteninhaberinnen/-inhabern zu erörtern. Die Maßnahmen nach Satz 2 sind für den in Rede stehenden Personenkreis regelmäßig zu wiederholen.

8 Aus- und Fortbildung

8.1 Auszug aus Nr. 8 der Richtlinie

8 Aus- und Fortbildung

Die Aus- und Fortbildungseinrichtungen nehmen das Thema "Korruptionsprävention" in ihre Programme auf. Hierbei ist vor allem der Fortbildungsbedarf der Führungskräfte, der Ansprechpersonen für Korruptionsprävention, der Beschäftigten in besonders korruptionsgefährdeten Arbeitsgebieten und der Beschäftigten der in Nr. 6 genannten Organisationseinheiten zu berücksichtigen.

8.2 Durchführungsbestimmungen

801. Die Berücksichtigung der Korruptionsprävention in der Aus-, Fort- und Weiterbildung soll den Angehörigen der Bundeswehr ein von ethischen Vorstellungen geprägtes Wertesystem vermitteln, die Auseinandersetzung mit dem Phänomen der Korruption ermöglichen, den geltenden Rechtsrahmen aufzeigen und sie aufgabengerecht für die Planung, Durchführung und Kontrolle entsprechender Vorkehrungen qualifizieren. Ergänzend zur Sensibilisierung und Belehrung nach Nr. 7 der Richtlinie zielen Qualifizierungsmaßnahmen insbesondere darauf ab, eine Reflektions- und Handlungskompetenz herzustellen, auf deren Basis die bewusste Vermeidung von Korruption Gegenstand dienstlichen Handelns wird.

802. Das BMVg entscheidet konzeptionell über die Verankerung von Inhalten der Korruptionsprävention in der Aus-, Fort- und Weiterbildung (zentrales Schulungsprogramm zur Korruptionsprävention). Bei dessen Gestaltung finden die Grundsätze der Empfehlungen zu Nr. 8 der Richtlinie Anwendung. Lehrgänge des zentralen Schulungsprogramms können in Abhängigkeit von ihrer Zielgruppe und der inhaltlichen Ausrichtung sowohl im Fernunterricht als auch in Präsenzform durchgeführt werden.

Daneben besteht im Falle der dienstlichen Notwendigkeit und im Rahmen verfügbarer Haushaltsmittel die Möglichkeit zur Teilnahme an sonstigen Qualifizierungsmaßnahmen, die das zentrale Schulungsprogramm bedarfsbezogen ergänzen oder vertiefen (z. B. Politische Bildung, Rechtsunterricht, In-House-Schulungen der Dienststellen, Seminare externer Bildungsträger). Zur Beurteilung eines ergänzenden oder vertiefenden Qualifizierungsbedarfs sind auch die im Rahmen der Dienst- und Fachaufsicht (vgl. Durchführungsbestimmungen zu Nr. 9 der Richtlinie) gewonnenen Erkenntnisse zugrunde zu legen. Bei der Organisation und Gestaltung von ergänzenden Qualifizierungsmaßnahmen sind die Ansprechpersonen für Korruptionsprävention ausdrücklich gehalten, sich fachlich einzubringen (Nr. 5.1 der Richtlinie).

803. Die Teilnahme an den im zentralen Schulungsprogramm eingerichteten Qualifizierungsmaßnahmen zur Wahrnehmung der Aufgaben einer Ansprechperson für Korruptionsprävention ist für diesen Personenkreis (einschließlich bestellter Stellvertretungen) obligatorisch. Werden Soldatinnen und Soldaten mit der Ausübung der Funktion einer Ansprechperson beauftragt, ist insoweit der Erwerb der ATN 1000237 vorzusehen. Seitens der Beschäfti- gungsstellen ist darauf hinzuwirken, dass möglichst zeitnah im Zusammenhang mit der Bestellung zur Wahrnehmung dieses Nebenamtes eine Einplanung der Betroffenen in die jeweiligen Lehrgänge erfolgt.

9 Konsequente Dienst- und Fachaufsicht

9.1 Auszug aus Nr. 9 der Richtlinie

9 Konsequente Dienst- und Fachaufsicht

9.1 Die Vorgesetzten üben ihre Dienst- und Fachaufsicht konsequent aus („Leitfaden für Vorgesetzte und Behördenleitungen"; Anlage 2). Dies umfasst eine aktive vorausschauende Personalführung und -kontrolle.

9.2 In diesem Zusammenhang achten die Vorgesetzten auf Korruptionssignale. Sie sensibilisieren regelmäßig und bedarfsorientiert ihre Mitarbeiterinnen und Mitarbeiter für Korruptionsgefahren.

9.2 Durchführungsbestimmungen

901. Eine konsequente Ausübung der Dienst- und Fachaufsicht einschließlich effektiver Kontrollen ist für die Korruptionsprävention von zentraler Bedeutung, da sie der Entstehung und dem Wachstum von Korruptionsstrukturen und Netzwerken entgegenwirkt (vgl. Nr. 402).

902. Die Aufsicht der Vorgesetzten im Rahmen der Korruptionsprävention umfasst neben der Prüfung von Recht- und Zweckmäßigkeit des fachlichen (Verwaltungs-)Handelns (Fachaufsicht) sowie der Beobachtung von Korruptionsindikatoren auch eine aktive und vorausschauende Mitarbeiterführung und Prüfung der persönlichen Pflichterfüllung der Beschäftigten (Dienstaufsicht); die Abgrenzung der Zuständigkeiten auf dem Gebiet des Personalwesens bleibt unberührt.

In besonders korruptionsgefährdeten Arbeitsgebieten ist die Kontrolltätigkeit intensiv durch fachliche Begleitung, Inanspruchnahme von Informationsrechten der Vorgesetzten und regel- mäßige Vorgangsprüfungen auszuüben. Dies gilt insbesondere dann, wenn bei Auftreten einer Verwendungsdauer von mehr als fünf Jahren eine Personalrotation nach Nr. 4.2 der Richtlinie oder eine Aufgabenrotation nicht durchgeführt werden kann und deshalb Ausgleichsmaßnahmen (vgl. Nr. 405) zu ergreifen sind.

903. Maßnahmen zur Korruptionsprävention unterliegen der Fachaufsicht durch vorgesetzte Dienststellen. Die Aufsicht ist grundsätzlich derart auszuüben, dass den Dienststellen eine Unterstützung zur Aufrechterhaltung und Verbesserung ihrer Vorkehrungen zur Korruptionsprävention ermöglicht wird und festgestellte Defizite beseitigt werden können. Hierzu sind regelmäßig örtliche Prüfungen durchzuführen, über deren Ergebnis die betreffende Dienststellenleitung zu unterrichten und zu dem ihr Gelegenheit zur Stellungnahme zu geben ist. Gegenstand dieser Prüfungen soll u.a. sein:

- Feststellung besonders korruptionsgefährdeter Arbeitsgebiete (Aktualität, Verfahren, sachgerechte Bewertungen),
- Durchführung von Risikoanalysen,
- Berücksichtigung des Mehr-Augen-Prinzips, Transparenz der Arbeitsabläufe,
- Ansprechperson für Korruptionsprävention (Bestellungsakt, Aktivitäten, Beteiligung durch die Dienststelle),
- Sensibilisierung (Art und Inhalt, Regelmäßigkeit, Dokumentation, Durchführung arbeitsplatzbezogener Belehrungen),
- Aus- und Fortbildung (Fortbildung der Ansprechperson und Stellvertretung, Maßnahmen für die Angehörigen der Dienststelle)
- Anwendung von Antikorruptionsklauseln,
- Anwendung des Verpflichtungsgesetzes,
- Annahme von Sponsoringleistungen und
- Entscheidungen im Zusammenhang mit der Annahme von Zuwendungen; Verhalten im Umgang mit Bewerbern, Bietern und Auftragnehmern.

Eine Überwachung der Präventionsmaßnahmen in den Gesellschaften mit Bundesbeteiligung nach Nr. 1.2 der Richtlinie erfolgt durch die Beteiligungsführung und die jeweiligen Kontroll- und Beschlussgremien der Unternehmen. Vorstehend aufgeführte Grundsätze sollen dabei berücksichtigt werden.

10 Unterrichtung und Maßnahmen bei Korruptionsverdacht

10.1 Auszug aus Nr. 10 der Richtlinie

10 Unterrichtungen und Maßnahmen bei Korruptionsverdacht

10.1 Bei einem durch Tatsachen begründeten Verdacht einer Korruptionsstraftat hat die Dienststellenleitung unverzüglich die Staatsanwaltschaft und die oberste Dienstbehörde zu unterrichten; außerdem sind behördeninterne Ermittlungen und vorbeugende Maßnahmen gegen eine Verschleierung einzuleiten.

10.2 Die obersten Bundesbehörden teilen jährlich dem Bundesministerium des Innern - auch für den jeweils nachgeordneten Bereich - in vorgegebener anonymisierter Form die Verdachtsfälle mit, in denen Verfahren eingeleitet wurden (untergliedert nach Bereich, Sachverhalt, eingeleiteten Maßnahmen) sowie den Ausgang der Verfahren, die im Berichtsjahr abgeschlossen wurden.

10.2 Durchführungsbestimmungen

B

1001. Ein Verdachtsfall ist gegeben, wenn tatsächliche Anhaltspunkte für eine Korruptions- straftat vorliegen bzw. bekannt werden. Solche Vorgänge sind – abweichend von Nr. 10.1 der Richtlinie – nach den Regelungen über besondere Vorkommnisse[14], über eine Abgabe an die Staatsanwaltschaft bei der Bearbeitung von Dienstvergehen[15] oder aufgrund sonstiger Weisungen unverzüglich an BMVg – R II 1 zu berichten.

Vor Unterrichtung von BMVg – R II 1 sind grundsätzlich keine dienststelleninternen Ermittlungen und vorbeugenden Maßnahmen gegen eine Verdunkelung bzw. Verschleierung durchzuführen, damit die notwendigen Untersuchungen koordiniert durchgeführt werden können. BMVg – R II 1 veranlasst die zur Aufklärung des Sachverhaltes und zur Verhinderung von Verdunkelungs- maßnahmen erforderlichen Schritte.

1002. Dienststelleninterne Beweissicherungsmaßnahmen kommen ausschließlich in Betracht, wenn nach Lage der Dinge ein sofortiges Einschreiten erforderlich ist, um den Verlust von mutmaßlich entscheidungserheblichen Beweismitteln zu verhindern (Gefahr im Verzug). Die Ansprechperson für Korruptionsprävention unterbreitet der Dienststellenleitung in diesen Fällen Vorschläge gegen eine Verdunkelung bzw. Verschleierung.

[14] BMVg – VR III 1 – Az 13 vom 14. Juli 1981 (Bundeswehrverwaltung und Rechtspflege, im VMBl nicht veröffentlicht), ZDv 10/13 Nr. 308 i. V. m. Anlage 8 (Streitkräfte)
[15] ZDv 14/3, B 117, Abschnitt IV, Nr. 3 i. V. m. Anlage 1 und 2.

1003. Die nach der Richtlinie geforderte unverzügliche Unterrichtung der Staatsanwaltschaft und die Abgabe an die Staatsanwaltschaft nach vorhergehenden Verwaltungsermittlungen wird allein durch BMVg – R II 1 sichergestellt.

Nr. 10.1 der Richtlinie i. V. m. Abschnitt II Nr. 2 Satz 1 bis 3 der Anlage 2 zur Richtlinie (Leitfaden für Vorgesetzte und Behördenleitungen) ist im Geschäftsbereich des BMVg insoweit nach Maßgabe vorstehender Grundsätze anzuwenden.

11 Leitsätze für die Vergabe

11.1 Auszug aus Nr. 11der Richtlinie

11 Leitsätze für die Vergabe

11.1 Wettbewerb

Der Grundsatz der öffentlichen Ausschreibung bzw. des offenen Verfahrens hat im Rahmen der Korruptionsprävention besondere Bedeutung.

Bei der Vergabe öffentlicher Aufträge ist regelmäßig im Rahmen der Dienst- und Fachaufsicht zu prüfen, ob unzulässige Einflussfaktoren vorgelegen haben.

11.2 Grundsätzliche Trennung von Planung, Vergabe und Abrechnung

Bei der Vergabe von öffentlichen Aufträgen nach den haushalts- und vergaberechtlichen Bestimmungen sind Vorbereitung, Planung und Bedarfsbeschreibung einerseits und die Durchführung des Vergabeverfahrens andererseits sowie möglichst auch die spätere Abrechnung grundsätzlich organisatorisch zu trennen.

11.3 Wettbewerbsausschluss

Die Dienststellen prüfen, ob schwere Verfehlungen von Bietern bzw. Bieterinnen oder Bewerbern bzw. Bewerberinnen vorliegen, die ihre Zuverlässigkeit in Frage stellen und die zum Ausschluss vom Wettbewerb führen können.

Eine solche schwere Verfehlung liegt insbesondere vor, wenn eine der genannten Personen demjenigen, der mit der Vorbereitung oder Durchführung eines Vergabeverfahrens befasst ist, einen Vorteil für diesen oder einen Dritten anbietet, verspricht oder gewährt.

11.2 Durchführungsbestimmungen

1101. Bei der Vergabe von öffentlichen Aufträgen sind Planung, Bedarfsbeschreibung, -priorisierung und -genehmigung einerseits und die Durchführung des Vergabeverfahrens andererseits sowie möglichst auch die spätere Abrechnung organisatorisch zu trennen. Dieser Grundsatz ist bereits anlässlich von konzeptionellen Überlegungen im Vorfeld von Organisationsmaßnahmen sowie generell bei der Festlegung von Zuständigkeiten und der Gestaltung von Arbeitsabläufen zu beachten (vgl. Nr. 3 und Nr. 9 der Richtlinie).

1102. Die Prüfung eines Wettbewerbsausschlusses von Bewerbern und Bietern richtet sich nach dem Erlass „*Verfahrensbestimmungen zur Prüfung von Unternehmen, deren Zuverlässigkeit wegen einer schweren Verfehlung in Frage steht*“[16].

[16] BMVg – ES – Az 76-05-01/001/02 vom 22. September 2003 (VMBl 2003 S. 150) in der Fassung BMVg – ES – Az 76-05-01/001/02 vom 23. März 2007 (VMBl 2007 S. 67)

12 Antikorruptionsklausel, Verpflichtungsgesetz

12.1 Auszug aus Nr. 12 der Richtlinie

12 Antikorruptionsklausel, Verpflichtung von Auftragnehmern oder Auftragnehmerinnen nach dem Verpflichtungsgesetz

12.1 Bei der Vergabe von öffentlichen Aufträgen sind in geeigneten Fällen Antikorruptionsklauseln vorzusehen.

12.2 Wirken private Unternehmen bei der Ausführung von Aufgaben der öffentlichen Hand mit, sind die einzelnen Beschäftigten dieser Unternehmen – soweit erforderlich – nach dem Verpflichtungsgesetz auf die gewissenhafte Erfüllung ihrer Obliegenheiten aus dem Auftrag zu verpflichten. Ein entsprechender Hinweis ist bereits in die jeweilige Ausschreibung aufzunehmen (einschließlich der Einforderung einer Bereitschaftserklärung). Den genannten Personen sind der „Verhaltenskodex gegen Korruption" (siehe Anlage 1) und ein Abdruck der geltenden Regelungen zur Annahme von Belohnungen und Geschenken auszuhändigen.

12.2 Durchführungsbestimmungen

1201. In den *„Zusätzlichen Vertragsbedingungen des Bundesministeriums der Verteidigung zur Verdingungsordnung für Leistungen Teil B (ZVB/BMVg)"*[17] sind Antikorruptionsklauseln enthalten. Die Antikorruptionsklauseln sind in ihrer jeweils geltenden Fassung in allen maßgeblichen Verträgen zu vereinbaren, in denen die Vergabestelle als öffentlicher Auftraggeber im Sinne von § 98 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB)[18] tätig wird.

1202. Potenzielle Bieter sind bereits in den Ausschreibungsunterlagen deutlich darauf hinzuweisen, dass der Vertrag eine Antikorruptionsklausel enthalten wird.

1203. Das Verpflichtungsgesetz ist nach Maßgabe der für den Geschäftsbereich des BMVg erlassenen Durchführungsbestimmungen[19] anzuwenden.

[17] VMBl 1998 S. 223, Änderung VMBl 2001 S. 154 bzw. BAnz. Nr. 34 vom 19. Februar 1998, Änderung BAnz. Nr. 96 vom 23. Mai 2001; Interimsfassung der Nrn. 11.4 und 11.5 ZVB/BMVg, Stand 28. Januar 2005.
[18] In der Fassung der Bekanntmachung vom 26. Juni 2013 (BGBl. I S. 1750, 3245), geändert durch Gesetz vom 7. August 2013 (BGBl. I S. 3154).
[19] BMVg – ES – Az 75-70-00/003/03 vom 20. August 2007 (VMBl 2007 S. 122)

13 Zuwendungen an Dienststellen, Sponsoring

13.1 Auszug aus Nr. 13 der Richtlinie

13 Zuwendungen zu Gemeinschaftsveranstaltungen und Gemeinschaftseinrichtungen; Sponsoring

Für die Annahme von Geld-, Sach- oder Dienstleistungen durch Private (Sponsoren) an eine oder mehrere Dienststellen des Bundes gilt die Allgemeine Verwaltungsvorschrift der Bundesregierung zur Förderung von Tätigkeiten des Bundes durch Leistungen Privater (Sponsoring, Spenden und sonstige Schenkungen) vom 7. Juli 2003 (BAnz. S. 14906).

13.2 Durchführungsbestimmungen

1301. Hinsichtlich der Annahme von Leistungen durch Dienststellen und Truppenteile der Bundeswehr ist der Erlass *Durchführungsbestimmungen zur „Allgemeinen Verwaltungsvorschrift der Bundesregierung zur Förderung von Tätigkeiten des Bundes durch Leistungen Privater (Sponsoring, Spenden und sonstige Schenkungen)“ für den Geschäftsbereich des Bundesministeriums der Verteidigung“*[20] in seiner jeweils geltenden Fassung anzuwenden.

[20] BMVg - ES – Az 75-11-15 vom 1. März 2011 (VMBl 2011 S. 37)

14 Zuwendungsempfänger

14.1 Auszug aus Nr. 14 der Richtlinie

14 Zuwendungsempfänger

14.1 Für Zuwendungen des Bundes im Rahmen institutioneller Förderungen ist der Zuwendungsempfänger durch besondere Nebenbestimmungen im Zuwendungsbescheid zu verpflichten, diese Richtlinie sinngemäß anzuwenden, wenn ihm durch Haushaltsrecht die Anwendung des Vergaberechts aufgegeben worden ist (Höhe der Zuwendung oder bei Finanzierung durch mehrere Stellen der Gesamtbetrag der Zuwendung mehr als 100.000 €). Bei Zuwendungsverträgen ist die entsprechende Anwendung der Richtlinie vertraglich zu vereinbaren.

14.2 Mit institutionellen Zuwendungsempfängern im Ausland sind vertraglich Grundsätze zur Korruptionsprävention zu vereinbaren.

14.2 Durchführungsbestimmungen

1401. Sofern ein Zuwendungsempfänger im Rahmen der institutionellen Förderung nach Anlage 1 zur VV Nr. 5.1 zu § 44 BHO[21] Vergaberecht anzuwenden hat und deshalb nach Nr. 14.1 der Richtlinie zu deren sinngemäßen Anwendung verpflichtet ist, haben die zuwendungsgebenden Stellen die in Anlage 3 der Empfehlungen enthaltene Musterklausel in den Zuwendungsbescheid aufzunehmen.

1402. Besteht für einen Zuwendungsempfänger im Rahmen der institutionellen Förderung nach vorgenannten Bestimmungen keine Verpflichtung zur Anwendung des Vergaberechts und somit auch nicht zur sinngemäßen Anwendung der Richtlinie, ist ihm von den zuwendungsgebenden Stellen nach Anlage 4 der Empfehlungen durch besondere Nebenbestimmung im Zuwendungsbescheid bzw. durch Vereinbarung im Zuwendungsvertrag die Einhaltung von Verhaltensstandards aufzugeben.

B **1403.** Im Rahmen des Zuwendungsverhältnisses sind die vom Zuwendungsempfänger nach Nr. 1401 und Nr. 1402 ergriffenen Maßnahmen zur Korruptionsprävention zu prüfen. Von den Zuwendungsempfängern sind hierzu im Sachbericht des Verwendungsnachweises die getroffenen Vorkehrungen darzulegen. Die zuwendungsgebenden Stellen der Bundeswehr können auf diese Prüfung verzichten, wenn innerhalb der Bundesregierung einem Ressort die Federführung für den institutionell geförderten Zuwendungsempfänger zugewiesen wurde und mit der federführenden Stelle Einvernehmen darüber besteht, dass die Korruptionsprävention des Zuwendungsempfängers insgesamt von dort sichergestellt wird. Die haushaltsrechtliche Prüfung des Verwendungsnachweises durch die zuwendungsgebende Stelle der Bundeswehr bleibt unberührt.

[21] Allgemeine Verwaltungsvorschriften zur Bundeshaushaltsordnung (VV-BHO) vom 14. März 2001 (GMBl 2001, S. 307), zuletzt geändert durch RdSchr. des BMF vom 3.9.2013 (GMBl. Nr. 50, S. 1002)

Signatures

Number of pages (including this one): 33

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this

Bundesministerium der Verteidigung

A-2100/2

Zentrale Dienstvorschrift

Annahme von Zuwendungen

Zweck der Regelung:	Sicherstellung eines rechtskonformen Vorgehens bei der Annahme von Zuwendungen
Herausgegeben durch:	Bundesministerium der Verteidigung
Beteiligte Interessenvertretungen:	Hauptpersonalrat beim BMVg, Gesamtvertrauenspersonenausschuss beim BMVg
Gebilligt durch:	Referatsleiter R III 2 ES
Herausgebende Stelle:	BMVg R III 1
Geltungsbereich:	Geschäftsbereich des Bundesministeriums der Verteidigung
Einstufung:	Offen
Einsatzrelevanz:	Ja
Berichtspflichten:	Ja
Gültig ab:	25.06.2020
Frist zur Überprüfung:	24.06.2025
Version:	1
Ersetzt:	• A-1400/7; • A-2100/20
Aktenzeichen:	60-15-01
Bestellnummer/DSK:	Entfällt

Inhaltsverzeichnis

1 Inhalt und Zweck der Regelung 3

2 Zuwendungskategorien 3

3 Zuwendungen an Angehörige des Geschäftsbereichs des Bundesministeriums der Verteidigung 4

3.1 Gesetzliche und externe Vorgaben 4
3.2 Grundsatz 4
3.3 Begriffsbestimmungen 4
3.4 Erfordernis der Zustimmung 6
3.4.1 Ausdrückliche Zustimmung 6
3.4.2 Nachträgliche Zustimmung 7
3.4.3 Stillschweigende Zustimmung 8
3.5 Zuständigkeiten und Verfahren 10
3.6 Rechtsfolgen von Verstößen 12
3.7 Nachweispflichten 12
3.8 Besondere Anzeigepflichten 12

4 Zuwendungen an Dienststellen und Truppenteile 12

4.1 Externe Vorgaben 12
4.2 Grundsatz 13
4.3 Begriffsbestimmungen 13
4.4 Rahmenbedingungen/Entscheidungsmaßstab 14
4.5 Zuständigkeiten und Verfahren 17
4.5.1 Sponsoring, Spenden und sonstige Schenkungen 17
4.5.2 Leistungen öffentlich-rechtlicher Körperschaften 19
4.5.3 Fälle/Veranstaltungen mit gleichgerichteter Zielsetzung bei angemessener Kostenteilung (Kooperationen im Sinne der Verwaltungsvorschrift Sponsoring) 20
4.6 Jährlicher Bericht 20

5 Anlagen 21

5.1 Rundschreiben zum Verbot der Annahme von Belohnungen oder Geschenken in der Bundesverwaltung des BMI D I 3 – 210 170/1 vom 8. November 2004 (GMBl 2004, S. 1074) 22
5.2 Allgemeine Verwaltungsvorschrift zur Förderung von Tätigkeiten des Bundes durch Leistungen Privater (Sponsoring, Spenden und sonstige Schenkungen) vom 7. Juli 2003 22
5.3 Textbausteine für Ablehnungen von Belohnungen oder Geschenken 22
5.4 Bezugsjournal 23
5.5 Änderungsjournal 23

1 Inhalt und Zweck der Regelung

101. Diese Zentrale Dienstvorschrift ergänzt und konkretisiert die gesetzlichen Regelungen und die Festlegungen der Bundesregierung zur Annahme von Belohnungen und Geschenken durch Bundesbedienstete sowie die Vorgaben über Förderung von Tätigkeiten des Bundes durch Leistungen Privater (Sponsoring, Spenden und sonstige Schenkungen). Sie dient damit der Unterstützung der Angehörigen des Geschäftsbereichs des Bundesministeriums der Verteidigung (GB BMVg) beim rechtssicheren Umgang mit der Annahme von Zuwendungen.

102. Übergreifender Zweck aller Regelungen über die Annahme von Zuwendungen ist es, bereits den Anschein fremder und sachwidriger Einflussnahme auf die Amtsführung zu vermeiden und die Integrität und Neutralität des Staates sowie seiner Bediensteten zu wahren.

2 Zuwendungskategorien

201. Die vorliegende Regelung erfasst jegliche Form von Zuwendungen im dienstlichen Zusammenhang.

202. Zuwendungen sind Leistungen, auf die kein Rechtsanspruch besteht. Sie sind zustimmungspflichtig.

203. Zu unterscheiden sind

- Zuwendungen an Angehörige des GB BMVg
  in Form von Belohnungen und Geschenken (siehe Abschnitt 3) sowie
- Zuwendungen an Dienststellen und Truppenteile
  in Form von Sponsoring, Spenden oder sonstigen Schenkungen (siehe Abschnitt 4).

204. Die Tatsache, dass Zuwendungen im Ergebnis einzelnen Angehörigen des GB BMVg zugutekommen (z. B. Eintrittskarten zu einer Veranstaltung), schließt nicht aus, dass es sich um Zuwendungen an die jeweilige Dienststelle handelt, sofern der Dienstherr über die interne Verteilung oder Nutzung der Zuwendung entscheidet.

205. Bestehen im Einzelfall Abgrenzungsschwierigkeiten, ob es sich um eine Zuwendung an Angehörige des GB BMVg oder an eine Dienststelle handelt, haben die für die Annahme von Belohnungen oder Geschenken zuständige Stelle, die für die Annahme von Zuwendungen an die Dienststelle zuständige Stelle sowie die zuständige Ansprechperson für Korruptionsprävention (APK) gemeinsam eine Entscheidung herbeizuführen.

3 Zuwendungen an Angehörige des Geschäftsbereichs des Bundesministeriums der Verteidigung

3.1 Gesetzliche und externe Vorgaben

301. Gemäß § 71 Abs. 1 des Bundesbeamtengesetzes, § 19 Abs. 1 des Soldatengesetzes und § 3 Abs. 2 des Tarifvertrages für den öffentlichen Dienst dürfen Belohnungen, Geschenke oder sonstige Vorteile in Bezug auf das Amt oder auf die dienstliche Tätigkeit grundsätzlich nicht angenommen werden. § 71 Abs. 1 des Bundesbeamtengesetzes und § 19 Abs. 1 des Soldatengesetzes beziehen dabei auch frühere Beamtinnen, Beamte, Soldatinnen und Soldaten mit ein. Ausnahmen bedürfen der Zustimmung.

302. Die für alle Bundesbedienstete geltenden Vorgaben zur Annahme von Belohnungen und Geschenken sind im Rundschreiben des Bundesministeriums des Innern (Rdschr. BMI) vom 08.11.2004 (siehe Anlage 5.1) geregelt.

303. Sofern in dieser Regelung keine abweichenden Vorgaben festgelegt sind, sind die Vorgaben des Rundschreibens des BMI vom 08.11.2004 zu beachten.

3.2 Grundsatz

304. Angehörige des GB BMVg müssen bereits jeden Anschein vermeiden, im Rahmen ihrer Amtsführung für persönliche Vorteile empfänglich zu sein und sollten daher von Anfang an jedem möglichen Interessenkonflikt aus dem Weg gehen, in den sie durch die Entgegennahme von Vorteilen geraten könnten.

305. Ausnahmen vom Verbot der Annahme von Belohnungen oder Geschenken kann es nur geben, wenn eine Beeinflussung der Angehörigen des GB BMVg nicht zu befürchten ist. Ausnahmen bedürfen der vorherigen Zustimmung des Dienstherrn oder des Arbeitgebers.

3.3 Begriffsbestimmungen

306. **Belohnungen oder Geschenke** sind **alle** Zuwendungen, auf die Angehörige des GB BMVg keinen Rechtsanspruch haben und durch die sie objektiv einen materiellen oder immateriellen Vorteil erlangen. Hierzu zählen auch Vorteile, die Dritten (insbesondere Angehörigen, Bekannten, dem eigenen Sportverein etc.) zugewendet werden, wenn sie bei den Beschäftigten zu einer Ersparnis führen oder diese in irgendeiner Weise tatsächlich besserstellen.

Neben Sachwerten können auch andere Leistungen, wie zum Beispiel[1]

- Einladungen zu Bewirtungen,
- Einladungen zu kostenlosen oder verbilligten Veranstaltungen,
- Honorarzahlungen,
- Preisverleihungen (sofern sie nicht seitens des Dienstherrn/Arbeitgebers erfolgen),
- die Übernahme von Reise- und Übernachtungskosten,
- Gutscheine, Eintritts- oder Freikarten,
- Vermittlung/Gewährung von Nebentätigkeiten bzw. Anschlusstätigkeiten,
- die Nutzung von Gegenständen (z. B. Pkw),
- die Mitnahme auf oder die Bezahlung von Urlaubsreisen oder
- Vergünstigungen bei Privatgeschäften (z. B. bei Krediten und Einkaufsmöglichkeiten)

als Zuwendungen an Angehörige des GB BMVg in Betracht kommen.

307. Sofern Angehörige des GB BMVg eine Leistung (z. B. Vortrag, Keynote-Speech, Panel- oder Workshopteilnahme) für einen Dritten erbringen und dafür von diesem die Reisekosten (Fahrt-, Flug- und/oder Unterbringungskosten) erstattet bekommen, handelt es sich **nicht um eine Zuwendung im Sinne dieser Regelung**, sondern vielmehr um einen Aufwandsersatz**.** Eine Annahme dieser Leistung ist in entsprechender Berücksichtigung des Bundesreisekostengesetzes (BRKG) erlaubt.

Übersteigen diese Leistungen bei überschlägiger Prognose im Vorfeld der Reise die Ansprüche aus dem BRKG in erheblichem Maß (um mehr als 25 Prozent), liegt die Annahme eines Geschenkes vor. Über die Annahme entscheidet dann die nach dieser Regelung zuständige Stelle nach Abschnitt 3.5.

308. In **Bezug auf das Amt** ist ein Vorteil gewährt, wenn die Vorteilsgeberin oder der Vorteilsgeber sich davon leiten lässt, dass die Angehörigen des GB BMVg ein bestimmtes Amt bekleiden oder bekleidet haben.

Beispiele: Ein Angehöriger des GB BMVg trägt im dienstlichen Auftrag auf der Veranstaltung eines Dritten vor. Dafür erhält er vom Veranstalter ein Geschenk.

Im Anschluss an eine Besprechung lädt der Vertreter eines Unternehmens den Projektverantwortlichen zu einem Abendessen ein.

Der Kommandeur einer Dienststelle erhält anlässlich seiner Verabschiedung in den Ruhestand ein Geschenk von einem Unternehmen, mit dem er die Jahre zuvor im dienstlichen Verkehr stand.

[1] Weitere Beispiele sind im Abschnitt II des Rdschr. BMI vom 08.11.2004 aufgeführt.

Für die Annahme von Geschenken aus dem Kreis der Angehörigen des GB BMVg im üblichen Rahmen (z. B. zum Geburtstag, Dienstjubiläum oder zur Verabschiedung) ist aufgrund des fehlenden Amtsbezuges keine Zustimmung erforderlich.

309. Eine **Annahme** eines Geschenkes oder einer Belohnung liegt bereits in jedem privaten oder dienstlichen Be- oder Ausnutzen. Dazu zählt auch, wenn der Vorteil unmittelbar an Dritte weiterverschenkt oder einer karitativen Einrichtung gespendet wird. Sie muss nicht ausdrücklich erklärt werden. Es reicht auch schlüssiges Verhalten.

Beispiele: Für eine dienstliche Autorentätigkeit bietet der Verlag, in dessen Zeitschrift der Artikel erscheint, der Autorin bzw. dem Autor ein Honorar an, welches diese bzw. dieser nicht selbst annehmen möchte, sondern den Verlag um direkte Überweisung an eine gemeinnützige Organisation bittet.

Ein Vertreter eines Unternehmens lässt nach einer Besprechung in der Dienststelle ein hochwertiges Modell eines von dem Unternehmen produzierten Fahrzeuges auf dem Besprechungstisch zurück. Es findet keine direkte Übergabe statt, seitens des beteiligten Angehörigen des GB BMVg wird das Modell aber auch nicht zurückgegeben.

310. Geschenke, die **von Repräsentantinnen und Repräsentanten anderer Staaten** an Angehörige des GB BMVg übergeben werden, sind in der Regel keine persönlichen Geschenke, sondern **Gastgeschenke** für die Bundesrepublik Deutschland. Die Gastgeschenke gehen unmittelbar in Staatseigentum über und sind zu vereinnahmen. Es besteht grundsätzlich für die Empfängerinnen und Empfänger dieser Gastgeschenke die Möglichkeit, das betreffende Gastgeschenk auf Antrag zu erwerben. Dies kann nur gegen Erstattung des ermittelten oder geschätzten Wertes an die zuständige Bundeskasse erfolgen.

Ein Gastgeschenk kann insbesondere dann als persönliches Geschenk gewertet werden, wenn es z. B. mit einer persönlichen Widmung oder Gravur für die Beschenkte oder den Beschenkten versehen ist oder z. B. als Dank für einen von der oder dem Beschenkten gehaltenen Vortrag oder eine vorgenommene Ausbildung übergeben worden ist. Im Zweifel gilt das Geschenk als Gastgeschenk für die Bundesrepublik Deutschland.

3.4 Erfordernis der Zustimmung

3.4.1 Ausdrückliche Zustimmung

311. Angehörige des GB BMVg dürfen eine Zuwendung erst annehmen, wenn die Zustimmung der zuständigen Stelle (siehe Abschnitt 3.5) vorliegt.

312. Die Entscheidung über die Erteilung der Zustimmung ist ausdrücklich und für jeden Einzelfall gesondert zu treffen. Sie erfolgt auf schriftlichen Antrag der bzw. des Angehörigen des GB BMVg und

ist dieser bzw. diesem schriftlich zu übermitteln. Angaben im Dienstreiseantrag oder bei der Reisekostenabrechnung ersetzen einen Antrag auf Zustimmung nicht.

313. Die Zustimmung zur Annahme kann nur erteilt werden, wenn aufgrund des Wertes oder der Beschaffenheit der Zuwendung oder sonstiger besonderer Umstände des Einzelfalls der Anschein der Empfänglichkeit der bzw. des Angehörigen des GB BMVg auszuschließen ist. Auf die subjektive Einstellung der Angehörigen des GB BMVg kommt es nicht an. In Zweifelsfällen ist die Zustimmung zu versagen[2].

314. Die Zustimmung kann auch unter einer Auflage erteilt werden. Als Auflage kommt z. B. die Entrichtung eines Geldbetrages, der in der Regel dem Verkehrswert der Zuwendung entspricht, an die Bundeskasse oder eine soziale Einrichtung in Betracht. Über die Auflage entscheidet die zuständige Stelle (siehe Abschnitt 3.5).

315. Die Annahme von Bargeld ist nicht genehmigungsfähig und hat auf jeden Fall zu unterbleiben. Ausnahme hiervon ist die Annahme von Honoraren für im dienstlichen Auftrag wahrgenommene Vortrags- und Autorentätigkeit und mit Ehrungen/Auszeichnungen verbundenen Preisgeldern; diese stehen in der Regel im vollen Umfang dem Dienstherrn zu.

316. Angehörige des GB BMVg, die im dienstlichen Verkehr mit Unternehmen oder Organisationen der Wirtschaft stehen, müssen in besonderer Weise den Anschein vermeiden, im Rahmen ihrer Amtsführung für persönliche Vorteile empfänglich zu sein. Sie haben daher bereits von sich aus die Annahme von Zuwendungen, für die keine stillschweigende Zustimmung erteilt ist (vgl. Abschnitt 3.4.3), grundsätzlich abzulehnen.

Beispiele: Annahme von Messekarten von Messeausstellern;

> Einladungen von Unternehmen und Organisationen der Wirtschaft zu Veranstaltungen oder Teilen von Veranstaltungen, die keinen dienstlichen Charakter haben (Eventveranstaltungen).

Sehen sich Angehörige des GB BMVg wegen der besonderen Umstände des Einzelfalls hierzu außerstande, haben diese die Zustimmung der zuständigen Stelle nach Abschnitt 3.5 einzuholen.

3.4.2 Nachträgliche Zustimmung

317. Sofern es nicht möglich ist, die erforderliche Zustimmung rechtzeitig einzuholen, darf die Zuwendung unter Vorbehalt angenommen werden. Die Zustimmung muss dann unverzüglich nachträglich eingeholt werden. Dabei sind die Gründe für die nachträgliche Beantragung anzugeben.

[2] Die Anlage 5.3 enthält Textbausteine, die Angehörigen des GB BMVg bei der Formulierung einer Ablehnung einer Belohnung oder eines Geschenks Unterstützung bieten.

318. Wird die nachträgliche Zustimmung abgelehnt, ist der Vorteil zurückzugeben. Ist eine Rückgabe unmöglich, ist durch die zuständige Stelle dessen üblicher Wert zu ermitteln und die ablehnende Entscheidung mit der Auflage zu verbinden, diesen Wert an die Vorteilsgeberin bzw. den Vorteilsgeber zu zahlen oder die Summe an soziale Einrichtungen zu spenden.

3.4.3 Stillschweigende Zustimmung

319. Die Zustimmung gilt in besonders gelagerten Fällen als erteilt (stillschweigende Zustimmung), sofern die Annahme nicht ausdrücklich von der zuständigen Stelle untersagt wurde:

3.4.3.1 Geringfügige Aufmerksamkeiten

320. Geringfügigkeit liegt dann vor, wenn der Verkehrswert (nicht der Herstellungswert) in der Bundesrepublik Deutschland 25 Euro nicht übersteigt. Die Annahme solcher Aufmerksamkeiten ist jedoch bei der zuständigen Stelle nach Abschnitt 3.5 anzuzeigen. Anzuzeigen sind der Gegenstand, der geschätzte Wert des Gegenstandes, der Anlass der Zuwendung und von wem der Gegenstand gewährt wurde.

321. Die Anzeigepflicht entfällt, wenn der Verkehrswert der Aufmerksamkeit fallbezogen höchstens 10 Euro beträgt.

322. Die Wertgrenzen beziehen sich dabei auf den Gesamtwert der Aufmerksamkeit, sofern diese aus mehreren Teilen besteht. Wird die Aufmerksamkeit mehreren Empfängerinnen bzw. Empfängern gewährt, kann der anteilige Wert als maßgeblich zugrunde gelegt werden.

323. Bei einer Häufung (in der Regel mehr als dreimal pro Kalenderjahr) von angezeigten Annahmen geringfügiger Aufmerksamkeiten desselben Vorteilsgebers bzw. derselben Vorteilsgeberin mit einem Wert zwischen 10 Euro und 25 Euro kann die zuständige Stelle für künftige Fälle die generelle Zustimmungsbedürftigkeit der Annahme derartiger Aufmerksamkeiten anordnen, wenn ansonsten der Anschein entsteht, im Rahmen der Amtsführung für persönliche Vorteile empfänglich zu sein.

324. Auf die Annahme von Aufmerksamkeiten mit einem Wert von über 25 Euro sollten Angehörige des GB BMVg von sich aus verzichten.

3.4.3.2 Geringfügige Dienstleistungen

325. Geringfügige Dienstleistungen, die die Durchführung eines Dienstgeschäftes erleichtern oder beschleunigen (z. B. Abholung mit einem Wagen vom Bahnhof), können von Angehörigen des GB BMVg angenommen werden. Die Geringfügigkeit ist hierbei an keine bestimmte Wertgrenze gebunden, sondern ist anhand der Umstände des Einzelfalls zu entscheiden.

3.4.3.3 Bewirtungen

326. Für die stillschweigende Zustimmung bei der Annahme von Bewirtungen gilt die Wertgrenze von 25 Euro nicht.

3.4.3.3.1 Bewirtungen durch Einrichtungen der öffentlichen Hand

327. Bewirtungen durch Einrichtungen der öffentlichen Hand können von Angehörigen des GB BMVg angenommen werden. Dies gilt auch bei Bewirtungen durch Zuwendungsgeber, die überwiegend von der öffentlichen Hand finanziert werden.

3.4.3.3.2 Bewirtungen durch Private im dienstlichen Zusammenhang

328. Angehörige des GB BMVg können an Bewirtungen durch Private aus Anlass oder bei Gelegenheit dienstlicher Handlungen, Besprechungen, Besichtigungen oder dergleichen teilnehmen, wenn sie **üblich und angemessen** sind oder wenn sie ihren Grund in den Regeln des Verkehrs und der Höflichkeit haben, denen sich auch Angehörige des öffentlichen Dienstes unter Berücksichtigung ihrer besonderen Verpflichtung zur objektiven Amtsführung nicht entziehen können, ohne gegen gesellschaftliche Formen zu verstoßen. Dies gilt nicht, wenn die Bewirtung nach Art und Umfang einen nicht unerheblichen Wert darstellt, wobei sich der Maßstab im Einzelfall auch an der amtlichen Funktion der Angehörigen ausrichtet.

329. Bewirtungen durch Private, die nicht aus Anlass oder bei Gelegenheit einer dienstlichen Handlung, sondern vielmehr vor bzw. nach der eigentlichen dienstlichen Handlung stattfinden und/oder lediglich der Kontaktpflege dienen (z. B. Abendessen), fallen nicht unter die stillschweigende Zustimmung. Ein dienstlicher Zusammenhang ist hier in der Regel nicht mehr gegeben. Angehörige des GB BMVg sollten daher grundsätzlich nur gegen Bezahlung an entsprechenden Bewirtungen teilnehmen. Sofern im Ausnahmefall ein dienstlicher Zusammenhang gesehen wird, ist bei Zustimmung der zuständigen Stelle nach Abschnitt 3.5 die Annahme der Bewirtung möglich.

3.4.3.3.3 Bewirtungen anlässlich allgemeiner Veranstaltungen

330. Angehörige des GB BMVg können Bewirtungen anlässlich allgemeiner Veranstaltungen, an denen sie im dienstlichen Auftrag oder mit Rücksicht auf die durch die Wahrnehmung ihrer Aufgaben auferlegten gesellschaftlichen Verpflichtungen teilnehmen (z. B. Einführung und/oder Verabschiedung von Amtspersonen, offizielle Empfänge) annehmen, wenn der Rahmen des **allgemein Üblichen und Angemessenen** nicht überschritten wird. Ansonsten ist zur Annahme der Bewirtung die Zustimmung der zuständigen Stelle nach Abschnitt 3.5 einzuholen.

3.4.3.4 Im Ausnahmefall als persönliches Geschenk zu wertendes Gastgeschenk

331. Sofern ein Gastgeschenk im Ausnahmefall als persönliches Geschenk zu werten ist (siehe dazu Nr. 310) und der Verkehrswert (nicht der Herstellungswert) in der Bundesrepublik Deutschland nicht mehr als 25 Euro beträgt, dürfen die oder der Beschenkte das Gastgeschenk behalten. Sie haben dies jedoch bei ihrer zuständigen Stelle nach den Nrn. 333, 334 oder 336 anzuzeigen, soweit der Verkehrswert 10 Euro übersteigt. Die Wertgrenzen beziehen sich dabei auf den Gesamtwert des Gastgeschenkes, sofern dieses aus mehreren Teilen besteht.

3.5 Zuständigkeiten und Verfahren

332. Die Zustimmung des Referates Recht III 1 ES (R III 1 ES) im BMVg ist erforderlich für

- die Annahme von Einladungen zu mehrtägigen kostenlosen oder verbilligten Veranstaltungen (z. B. Lehrgängen, Seminaren oder sonstigen Fortbildungsveranstaltungen) von Unternehmen der Wirtschaft; bei bis zu eintägigen Veranstaltungen bleibt es bei der Zuständigkeit der in der Nr. 334 genannten Vorgesetzten,
- die Benutzung von Firmenluftfahrzeugen,
- die mehrmalige, nicht nur gelegentliche unentgeltliche Benutzung oder Mitbenutzung von Firmenfahrzeugen. In diesem Zusammenhang wird darauf hingewiesen, dass die gelegentliche Mitbenutzung eines Firmenfahrzeugs, das ohnehin zum oder vom Geschäftsort verkehrt (z. B. Abholfahrten), bereits im Dienstreiseantrag anzugeben oder – bei unvorhergesehenen Fahrten – der oder dem jeweiligen Vorgesetzten nachträglich anzuzeigen ist,
- die Annahme von Honoraren für im dienstlichen Auftrag wahrgenommene Vortrags- oder Autorentätigkeiten,
- die Annahme von Preisgeldern/geldwerten Zuwendungen (z. B. Gutscheinen) im Rahmen von Ehrungen, Auszeichnungen und Preisverleihungen sowie
- Fälle von besonderer Bedeutung (z. B. Fälle mit besonderer Außenwirkung [Annahme von Zuwendungen von Auftragnehmern, die aufgrund von (strafrechtlichen) Vorwürfen im Mittelpunkt von Presseberichterstattungen stehen]).

Im Antrag auf Zustimmung an das Referat R III 1 ES im BMVg ist die Personalnummer anzugeben. Bei der Annahme von Honoraren und Preisgeldern sind darüber hinaus folgende Angaben erforderlich:

- die Bestätigung des dienstlichen Interesses durch die Vorgesetzte oder den Vorgesetzten sowie
- die Angabe über den prozentualen Anteil der Ausarbeitung des Artikels/des Vortrags/der dem Preisgeld zugrundeliegenden Ausarbeitung im Dienst bzw. in der Freizeit.

333. Die Befugnis, über die Annahme von Belohnungen oder Geschenken zu entscheiden, die Angehörigen des BMVg in Bezug auf ihr Amt oder ihre dienstliche Tätigkeit gewährt werden sollen, obliegt dem zuständigen Personalreferat in der Abteilung Personal im Ministerium oder im Bundesamt

für das Personalmanagement der Bundeswehr. Ausnahmen davon sind in den Internen Regelungen des Bundesministeriums der Verteidigung Teil II (IR BMVg Teil II)[3] aufgeführt.

334. In allen anderen Fällen obliegt die Befugnis, über die Annahme von Belohnungen oder Geschenken zu entscheiden, die Angehörigen des GB BMVg in Bezug auf ihr Amt oder ihre dienstliche Tätigkeit gewährt werden sollen, als zuständige Stelle im Sinne der Nr. 311

a) für Beamtinnen und Beamte der Leitung der Beschäftigungsdienststelle,
b) für Richterinnen und Richter den Präsidentinnen oder Präsidenten der Truppendienstgerichte,
c) für Soldatinnen und Soldaten der oder dem nächsthöheren Disziplinarvorgesetzten und
d) für Arbeitnehmerinnen und Arbeitnehmer der Leitung der Beschäftigungsdienststelle.

Für Entscheidungen nach Beendigung des Arbeits- oder Dienstverhältnisses sind die nach den Buchstaben a) bis d) zuletzt entscheidungsbefugten Vorgesetzten bzw. deren Nachfolger im Amt zuständig. Sollten in Folge von Umstrukturierungsmaßnahmen oder Auflösungen von Dienststellen frühere Unterstellungsverhältnisse nicht mehr gegeben sein, geht die Entscheidungsbefugnis auf die dann für den durch die Beschenkte bzw. den Beschenkten ehemals wahrgenommenen Aufgabenbereich zuständigen Vorgesetzten über.

335. Die Ausübung der Befugnis kann an entsprechend geschulte Angehörige der Dienststelle delegiert werden. Dies gilt nicht für die unter Nr. 334, c) genannten Vorgesetzten. Die Schulung sollte möglichst durch die für die Dienststelle zuständige APK erfolgen.

336. Die Nr. 333 gilt auch für den in Nr. 334 genannten Personenkreis (Leitung der Beschäftigungsdienststelle/Präsidentinnen oder Präsidenten der Truppendienstgerichte) sowie für Soldatinnen und Soldaten des nachgeordneten Bereiches, für die die Bundesministerin bzw. der Bundesminister der Verteidigung nächsthöhere Vorgesetzte bzw. nächsthöherer Vorgesetzter ist.

337. Die nach dieser Regelung festgelegte Anzeigepflicht ist gegenüber der gleichen Stelle wahrzunehmen, die für die Zustimmung über die Annahme von Belohnungen oder Geschenken zuständig wäre.

338. Die Entscheidung über die Verwendung von Gastgeschenken und über die Festlegung des Gegenwertes bei möglichem Erwerb durch die Empfängerinnen und Empfänger trifft die nach den Nrn. 333, 334 oder 336 zuständige Stelle.

[3] Die IR BMVg Teil II sind im Intranet BMVg zusammen mit der ergänzenden Geschäftsordnung des BMVg unter den Grundlagendokumenten veröffentlicht.

3.6 Rechtsfolgen von Verstößen[4]

339. Der Verstoß gegen das Verbot der Annahme von Belohnungen oder Geschenken stellt ein Dienstvergehen bzw. eine Verletzung arbeitsvertraglicher Pflichten dar und hat dienst- und arbeitsrechtliche sowie ggf. strafrechtliche Konsequenzen.

3.7 Nachweispflichten

340. Die Anzeigen, die Anträge und die entsprechenden Bescheide sind zur jeweiligen Personalakte der Beschäftigten zu nehmen. Die nach dieser Regelung zuständigen Vorgesetzten lassen der personalbearbeitenden Stelle eine Ausfertigung der Entscheidung zukommen.

341. Im Rahmen der Dienstaufsicht haben die für die Genehmigung zuständigen Dienststellen der Bundeswehr einen zentralen Nachweis über die nach dieser Regelung getroffenen Entscheidungen und eingegangenen Anzeigen zu führen. Dies schließt die Prüfung ein, ob die stillschweigende Zustimmung für bestimmte Einzelfälle zu widerrufen ist. Dadurch soll der Gefahr vorgebeugt werden, dass durch die Annahme derartiger Vorteile der Eindruck der Bevorzugung Einzelner oder der Befangenheit entsteht. Hierbei ist gegebenenfalls auch die Häufung von Zuwendungen zu berücksichtigen.

3.8 Besondere Anzeigepflichten

342. Alle Angehörigen des GB BMVg haben die Pflicht, ihre Vorgesetzten über jeden Versuch, ihre Tätigkeit durch ein Angebot von Geschenken oder Belohnungen zu beeinflussen, unverzüglich zu unterrichten. Der bzw. die Angehörige oder der bzw. die Vorgesetzte haben in diesem Fall auch die zuständige APK zu unterrichten.

343. Auf die Pflicht, anlässlich von Dienstreisen in der Reisekostenabrechnung Angaben über die Übernahme von Leistungen Dritter (Übernahme von Fahrtkosten, Gewährung unentgeltlicher Verpflegung und Unterkunft) zu machen, wird besonders hingewiesen.

4 Zuwendungen an Dienststellen und Truppenteile

4.1 Externe Vorgaben

401. Die für alle Dienststellen des Bundes und für die Streitkräfte geltenden Vorgaben zur Förderung von Tätigkeiten des Bundes durch Leistungen Privater (Sponsoring, Spenden und sonstige Schenkungen) sind in einer Allgemeinen Verwaltungsvorschrift des BMI vom 7. Juli 2003 (VV Sponsoring; siehe Anlage 5.2) geregelt und zu beachten.

[4] Vgl. Abschnitt V des Rdschr. BMI vom 08.11.2004.

402. Die VV Sponsoring findet für alle unentgeltlichen Leistungen Privater an eine Dienststelle oder einen Truppenteil, mit der eine Tätigkeit im GB BMVg mit dem Ziel gefördert wird, dadurch einen werblichen oder sonst öffentlichkeitswirksamen Vorteil zu erreichen, **direkte Anwendung** (Sponsoring). Für (andere) unentgeltliche Zuwendungen Privater (insbesondere für Spenden und sonstige Schenkungen) an eine Dienststelle oder einen Truppenteil, für die eine Gegenleistung weder erwartet noch erbracht wird, gelten die Regelungen der VV Sponsoring **sinngemäß**.

403. Die nachfolgenden Vorgaben dieser Zentralen Dienstvorschrift finden für alle Zuwendungen an Dienststellen (Sponsoring, Spenden und sonstige Schenkungen) Anwendung, sofern sich die Vorgabe nicht ausdrücklich auf Sponsoring beschränkt.

4.2 Grundsatz

404. Öffentliche Ausgaben sind durch Haushaltsmittel zu finanzieren. Zuwendungen an Dienststellen und Truppenteile durch Private kommen daher nur ergänzend in Betracht und sind transparent zu machen. Mit dieser Regelung sollen die parlamentarische Budgethoheit gewahrt und die Unabhängigkeit und Eigenständigkeit der Verwaltung gegenüber privaten Mittelgebern gesichert werden. Um die Integrität und Neutralität des Staates zu wahren, muss schon jeder Anschein fremder Einflussnahme auf die Aufgabenwahrnehmung vermieden werden.

4.3 Begriffsbestimmungen

405. **Sponsoring** ist eine Vereinbarung, die sowohl Leistungen des Sponsors als auch Leistungen des Gesponserten beinhaltet. Durch Zuwendung von Geld-, Sach- oder Dienstleistungen an Dienststellen und Truppenteile fördert der private Sponsor eine Tätigkeit der Verwaltung/der Streitkräfte mit dem Ziel, dadurch einen werblichen oder sonst öffentlichkeitswirksamen Vorteil zu erreichen. Mit der Gewährung der Zuwendungen werden regelmäßig auch eigene unternehmensbezogene Ziele der Werbung oder der Öffentlichkeitsarbeit des Sponsors verfolgt. Beim Sponsoring wird eine Partnerschaft eingegangen, bei der beide Parteien Vorteile für die eigenen Interessen bzw. Aufgaben erzielen wollen.

Beispiel: Der Tag der offenen Tür einer Dienststelle wird mit Mitteln ortsansässiger Firmen unterstützt. Als Leistung der Dienststelle werden die Logos der Firmen auf das Programm, welches an die Besucher verteilt wird, gedruckt.

406. **Spenden** sind freiwillige Leistungen **zur Förderung steuerbegünstigter Zwecke**. Sie sind keine Gegenleistung für eine bestimmte Leistung des Empfängers und stehen nicht in einem tatsächlichen wirtschaftlichen Zusammenhang mit dessen Leistungen.

Beispiel: Das Militärhistorische Museum der Bundeswehr erhält von einem privaten Sammler zur Ergänzung der musealen Sammlung ein Ausstellungsstück. Der private Sammler erwartet keine Gegenleistung. Das Militärhistorische Museum der Bundeswehr verfolgt mit der Förderung von Kultur gemeinnützige Zwecke.

407. Mit dem Begriff „**sonstige Schenkungen**“ sind andere Zuwendungen ohne Gegenleistung gemeint; neben Schenkungen im zivilrechtlichen Sinne – darunter vor allem mäzenatische Schenkungen – kommen z. B. Erbeinsetzungen und Vermächtnisse in Betracht.

Beispiel: Ein Hersteller von Heizungstechnik übergibt einer Dienststelle mit Ausbildungswerkstatt kostenlos Heizgeräte zu Ausbildungszwecken. Eine Leistung an die Firma erbringt die Dienststelle nicht.

Unter den Begriff sonstige Schenkungen fallen auch Zuwendungen an Dienststellen und Truppenteile, die nicht der Erfüllung dienstlicher Aufgaben dienen, sondern in Anerkennung für geleistete Dienste oder als symbolisches Zeichen der Verbundenheit erfolgen, und für die eine Gegenleistung weder erwartet noch erbracht wird.

408. **Private** im Sinne der vorliegenden Regelung können unter anderem Unternehmen, (gemeinnützige) Vereine, (Berufs-)Verbände oder natürliche Personen sein. Die Vorgaben gelten auch für Leistungen an die dem GB BMVg zugehörenden Personal- und Interessenvertretungen, die Gleichstellungsbeauftragten, die Betriebssportgruppen oder ähnliche Einrichtungen.

409. **Leistungen öffentlich-rechtlicher Körperschaften** (Zuwendungen öffentlicher Stellen) zur Förderung von Tätigkeiten des Bundes an Dienststellen oder Truppenteile sind keine Leistung im Sinne der VV Sponsoring und dieser Regelung. Das gilt z. B. für Leistungen von

- öffentlich-rechtlichen überstaatlichen Einrichtungen,
- Behörden des Bundes (z. B. oberste Bundesbehörden, weitere Behörden der unmittelbaren und mittelbaren Bundesverwaltung, Gerichte des Bundes, Streitkräfte),
- Behörden der Länder und Gemeinden oder
- sonstigen öffentlichen Institutionen (z. B. Sparkassen, gesetzliche Krankenkassen als Körperschaften des öffentlichen Rechts (§ 4 Abs. 1 Sozialgesetzbuch (SGB) V), öffentlich-rechtliche Sendeanstalten), gesetzliche Träger der Renten- und Unfallkassen.

Beispiel: An einem Standort wird ein Tag der offenen Tür durchgeführt. Die örtliche Sparkasse unterstützt durch die Aufstellung einer Hüpfburg.

410. Fälle der **gleichgerichteten Zielsetzung bei angemessener Kostenteilung** sind kein Sponsoring im Sinne der VV Sponsoring und dieser Regelung. Deren Vorgaben gelten daher nicht, wenn der Private und die Dienststelle oder der Truppenteil (z. B. bei Veranstaltungen) gleichgerichtete Ziele bei angemessener Kostenteilung verfolgen.

4.4 Rahmenbedingungen/Entscheidungsmaßstab

411. Da öffentliche Ausgaben durch Haushaltsmittel zu finanzieren sind, dürfen Dienststellen und Truppenteile Geld-, Sach- oder Dienstleistungen Privater grundsätzlich nicht annehmen.

412. In Ausnahmefällen dürfen Leistungen nach Nr. 411 angenommen werden, wenn ein dienstliches Interesse an der Annahme der Zuwendung besteht und jegliche fremde Beeinflussung der Aufgabenerfüllung der Dienststelle bzw. des Truppenteils oder jeder Anschein einer solchen Beeinflussung ausgeschlossen ist. Die Annahme der Leistung bedarf der **Zustimmung**.

413. Als Ausnahmefälle können insbesondere in Betracht kommen:

a) Unterstützung von Dienststellen und Truppenteilen im Auslandseinsatz oder im Rahmen von Missionen im Ausland[5], jeweils als Ergänzung des dienstlich bereitgestellten Betreuungsangebots, sofern mit der Zuwendung die Verbundenheit mit der Truppe im Einsatzgebiet dokumentiert oder besondere Anlässe gewürdigt werden sollen.
b) Ergänzung des dienstlich bereitgestellten Fortbildungsangebots.
c) Unterstützung von Veranstaltungen im Sinne der Öffentlichkeitsarbeit.
d) Unterstützung von Maßnahmen der Familienbetreuungszentren und -stellen.
e) Unterstützung von Maßnahmen des Personalmarketings.
f) Unterstützung der Durchführung von Wettbewerben des Kontinuierlichen Verbesserungsprogramms in der Bundeswehr (KVP).
g) Unterstützung der Durchführung sportlicher Veranstaltungen mit externer Beteiligung.
h) Unterstützung der Betreuung bzw. Therapie einsatzgeschädigter Soldatinnen und Soldaten.

414. Die Annahme von Zuwendungen für **interne Veranstaltungen oder Maßnahmen** (z. B. Kameradschaftsabende oder Jahresabschlussfeiern) ist ausgeschlossen. Veranstaltungen, an denen neben dem Personal des GB BMVg lediglich dessen Familienangehörige teilnehmen, sind interne Veranstaltungen. Das Verbot der Annahme von Zuwendungen für interne Veranstaltungen gilt nicht für Maßnahmen nach Nr. 413, a) bis f) und h).

415. Für interne Veranstaltungen geselliger Art **mit beschränkter Beteiligung der Öffentlichkeit**, insbesondere für Bälle, kann die Annahme von Zuwendungen vor dem Hintergrund der Öffentlichkeitsarbeit zulässig sein, es dürfen aber keine Zuwendungen von Auftragnehmern der Bundeswehr angenommen werden.

416. Der Einsatz von Sponsoring sollte im Umfang und Häufigkeit grundsätzlich **restriktiv** erfolgen. Das Kriterium der **„ergänzenden“** bzw. **„unterstützenden“** Leistung muss auf den jeweiligen Einzelfall bezogen betrachtet und bewertet werden. Es bieten sich beispielsweise folgende Bezugsgrößen an:

Durchführung einer Veranstaltung:	Gesamtkosten der Veranstaltung;
Bereitstellung von Material für die Ausbildung:	Haushaltsmittelansatz auf dem Aus- und Fortbildungstitel der Dienststelle

[5] Vgl. Zentrale Dienstvorschrift A-110/1 VS-NfD „Anerkennung von Verwendungen als Missionen“.

417. In der **Eingriffsverwaltung** ist die Annahme von Zuwendungen nicht zulässig. Dies bringt zum Ausdruck, dass Dienststellen zur Erfüllung ihrer hoheitlichen Aufgaben keine Leistungen annehmen dürfen.

418. Die Integrität und Neutralität des Staates muss gewahrt und eine Beeinflussung der Streitkräfte/Verwaltung bei ihrer Aufgabenwahrnehmung ausgeschlossen werden. Die **Vermeidung des Anscheins fremder Einflussnahme** bei der Annahme von Zuwendungen ist wegen der Vorbildfunktion der öffentlichen Verwaltung/der Streitkräfte und des Vertrauens in sie Grundvoraussetzung für die Zulässigkeit der Annahme von Leistungen. Ist die Vermeidung dieses Anscheins nicht gewährleistet, dürfen Leistungen nicht angenommen werden.

Vor jeder Annahme von Leistungen muss geprüft werden, ob Beziehungen mit/zu dem Geber bestehen oder möglicherweise angestrebt werden, die zu einem Interessenkonflikt oder schon zum Anschein eines Interessenkonfliktes durch die Leistungsannahme führen könnten. Insbesondere dann, wenn Entscheidungen zu Geschäftsbeziehungen anstehen, sollten keine Leistungen von Gebern angenommen werden, die von dieser Entscheidung betroffen sind.

Auch wenn solche Beziehungen nicht bestehen, können gleichwohl durch die Annahme von Leistungen Beziehungen entstehen, die geeignet sind, zumindest den Anschein zu erwecken, dass ein öffentlicher Wettbewerb eingeschränkt oder ausgeschlossen ist.

419. Die Wettbewerbs- und Chancengleichheit potenzieller Sponsoren ist zu wahren. Das **Prinzip der Wettbewerbs- und Chancengleichheit** ist auch dann zu beachten, wenn sich ein Unternehmen wiederholt eigeninitiativ als Sponsor anbietet.

420. Bei der Auswahl des Sponsors ist auf Objektivität und Neutralität zu achten. Die **Auswahl der Sponsoren** soll möglichst breit angelegt sein. Soweit möglich, soll eine größere Anzahl von Sponsoren angesprochen und ihnen die Gelegenheit zu Angeboten von Sponsoringleistungen gegeben werden. Unternehmen, die in einem regionalen Bezug zu der beantragenden Dienststelle oder dem Truppenteil stehen, sind möglichst am Auswahlverfahren zu beteiligen. Dazu sind geeignete kommunikative Möglichkeiten (z. B. auch ein Internetauftritt der Dienststelle) auszuschöpfen. Von „informellen Anfragen“ an potenzielle Sponsoren ist zur Sicherstellung des Wettbewerbs abzusehen.

421. Der Anschein einer Abhängigkeit von einzelnen Zuwendungsgebern ist zu vermeiden. Dies gilt insbesondere für Firmen, die in erheblichem Umfang Auftragnehmer der Bundeswehr sind.

422. Die Annahme von Zuwendungen durch Dienststellen oder Truppenteilen von

- Beteiligungsgesellschaften des Bundes oder
- institutionellen Zuwendungsempfängern, auch wenn diese nur teilweise aus dem Bundeshaushalt finanziert werden,

ist nicht zulässig.

423. Vor der Annahme von Leistungen ist sicherzustellen, dass für dadurch anfallende Folgeausgaben (z. B. Wartungskosten, Betriebskosten etc.) Haushaltsmittel zur Verfügung stehen.

4.5 Zuständigkeiten und Verfahren

4.5.1 Sponsoring, Spenden und sonstige Schenkungen

424. Sponsoringbeauftragte bzw. Sponsoringbeauftragter für den GB BMVg ist die Referatsleitung R III 1 im BMVg.

425. Die für Fragen des Sponsorings und insbesondere für die Zustimmung zur Annahme von Sponsoringleistungen zuständige Stelle im Sinne von Nr. 3.3 der VV Sponsoring ist das Referat R III 1 ES im BMVg, soweit die Zuständigkeit nach den folgenden Vorgaben nicht auf eine andere Stelle übertragen wurde.

426. Über Leistungen in den Fällen nach Nr. 413, a) bis f), die den Betrag von 500 Euro pro Maßnahme/Veranstaltung (z. B. Tag der offenen Tür) nicht überschreiten, entscheidet die Leitung der Dienststelle oder des Truppenteils, die oder der die Leistung erhalten soll.

427. In den Fällen nach Nr. 413, g) und h) entscheidet die jeweilige Leitung der Dienststelle oder des Truppenteils, die oder der die Leistung erhalten soll, wenn die Leistungen den Betrag von 1 000 Euro pro Maßnahme nicht überschreiten.

428. Über die Annahme von Zuwendungen an Dienststellen und Truppenteile, die nicht der Erfüllung dienstlicher Aufgaben dienen, sondern in Anerkennung für geleistete Dienste oder als symbolisches Zeichen der Verbundenheit erfolgen, und für die eine Gegenleistung weder erwartet noch erbracht wird, entscheidet die Leitung der Dienststelle, die der Dienststelle oder dem Truppenteil, die oder der die Leistung erhalten soll, vorgesetzt ist, wenn die Leistungen den Betrag von 500 Euro pro Maßnahme nicht überschreiten.

Bei der Entscheidung ist der ggf. erforderliche Verteilerschlüssel (z. B. bei der Annahme von Freikarten) festzulegen[6].

Beispiele: Dem Kommandanten einer seegehenden Einheit werden fünf Freikarten für ein Konzert mit einem Gesamtwert von 350 Euro angeboten. Die Leitung der vorgesetzten Dienststelle stimmt der Annahme zu und legt fest, dass die Freikarten im Losverfahren unter allen Besatzungsmitgliedern verteilt werden.

Ein Förderverein möchte zur Gestaltung des Aufenthaltsraums einer Dienststelle beitragen und einen Tischkicker finanzieren. Die Leitung der vorgesetzten Dienststelle

[6] Die Leitungen der dem BMVg direkt nachgeordneten Dienststellen entscheiden bis zu der festgelegten Wertgrenze selbst über die Annahme solcher Zuwendungen an ihre Dienststelle.

stimmt der Annahme zu und legt fest, dass der Tischkicker in den Bestand der Dienststelle zu vereinnahmen ist.

429. Die Annahme von Leistungen an Dienststellen oder Truppenteile ist von der Leitung der Dienststelle oder des Truppenteils, die oder der die Leistung erhalten soll, **auf dem Dienstweg** beim Referat R III 1 ES im BMVg zu beantragen. Dies gilt nicht für die Fälle nach den Nrn. 426, 427 und 428.

430. In dem Antrag sind die die Ausnahme begründenden Umstände und das dienstliche Interesse an der Annahme der Leistung darzulegen. Der Antrag ist auf dem Dienstweg vorzulegen und muss die Stellungnahme aller beteiligten Dienststellen zum dienstlichen Interesse an der Annahme der Leistung enthalten. Bei Zuwendungen an Dienststellen und Truppenteile, die nicht der Erfüllung dienstlicher Aufgaben dienen, sondern in Anerkennung für geleistete Dienste oder als symbolisches Zeichen der Verbundenheit erfolgen, und für die eine Gegenleistung weder erwartet noch erbracht wird, ist bei der Antragstellung die Begründung des dienstlichen Interesses an der Annahme nicht erforderlich und eine Befürwortung der Annahme durch alle beteiligten Dienststellen ausreichend. Der Antrag soll **spätestens acht Wochen** vor der geplanten Annahme der Leistung beim Referat R III 1 ES im BMVg eingehen.

431. Eine verspätete oder unvollständige Antragstellung kann zur Ablehnung des Antrags führen. Wird eine Leistung Privater ohne die nach Nr. 412 erforderliche Zustimmung angenommen, kann durch das Referat R III 1 ES im BMVg eine Rückabwicklung der Leistung bei gleichzeitiger Einleitung einer Schadensbearbeitung angeordnet werden.

432. Der Zuwendungsgeber bzw. die Zuwendungsgeberin muss schriftlich sein bzw. ihr Einverständnis erklären, dass sein bzw. ihr Name, sein bzw. ihr Wohnort oder Firmensitz, seine bzw. ihre Leistung und deren Wert im Sponsoringbericht des BMI aufgeführt werden und dass Betriebs- oder Geschäftsgeheimnisse einer Veröffentlichung nach dem Informationsfreiheitsgesetz nicht entgegenstehen.[7]

433. Ab einer Zuwendung mit einem Wert von über 5 000 Euro ist mit der Zuwendungsgeberin bzw. dem Zuwendungsgeber ein schriftlicher Vertrag[8] abzuschließen. Die Einverständniserklärung nach Nr. 432 ist dann Bestandteil des Vertrages (§ 6 Abs. 4 der Mustervereinbarung).

434. Als Verpflichtung der Dienststelle darf ausschließlich die Darstellung des Sponsors zugelassen werden, insbesondere die mündliche oder schriftliche Nennung des Namens, der Firma und der Marke des Sponsors sowie die Präsentation seines Logos und sonstiger Kennzeichen im Rahmen der Veranstaltung. Über diese Verpflichtung hinaus darf die Dienststelle den Sponsor und seine Erzeugnisse nicht öffentlich anpreisen.

---

[7] Einverständniserklärung, siehe Formular-Management-System (FMS)-Formularnummer Bw-5132.

[8] Muster „Sponsoringvereinbarung“, siehe FMS-Formularnummer Bw-2933. Einzelfallabhängig ist zu prüfen, ob und inwieweit die Bestimmungen der Mustervereinbarung angemessen sind. Formulierungen sind ggf. anzupassen (z. B. bei Spenden und sonstigen Schenkungen).

Die Annahme einer Spende oder einer sonstigen Schenkung liegt nur dann vor, wenn von dem Privaten keine Gegenleistung (z. B. in Form einer Logo-Präsentation) erwartet und von der Dienststelle erbracht wird.

435. In den Fällen der Nrn. 426, 427 und 428 ist von der zuständigen Stelle ein Vermerk zu fertigen. Um dem Transparenzgebot gerecht zu werden, sind schriftlich der Verwendungszweck, der Wert der Leistung, der Name des Gebers bzw. der Geberin und vereinbarte Verpflichtungen/Gegenleistungen der Dienststelle festzuhalten. Mit der nach Nr. 432 erforderlichen Einverständniserklärung der Zuwendungsgeberin bzw. des Zuwendungsgebers ist dieser zu den Akten zu nehmen.

436. Einnahmen aus Sponsoring- oder anderen Leistungen sind bei Kapitel 1411 Titel 282 09 wie folgt zu buchen:

- Buchungsabschnitt 001: Zuwendungen Dritter durch Sponsoring;
- Buchungsabschnitt 002: Zuwendungen Dritter durch Spenden;
- Buchungsabschnitt 003: Geldspenden an die Bundeswehr für humanitäre Hilfeleistungen;
- Buchungsabschnitt 005: Zuwendungen Dritter durch andere freiwillige Geldleistungen.

Ausgaben aus Sponsoring- oder anderen Leistungen sind bei Kapitel 1411 Titel 547 09 wie folgt zu buchen:

- Buchungsabschnitt 001: Ausgaben aufgrund Zuwendungen Dritter durch Sponsoring;
- Buchungsabschnitt 002: Ausgaben aufgrund Zuwendungen Dritter durch Spenden:
- Buchungsabschnitt 003: Ausgaben aus Geldspenden an die Bundeswehr für humanitäre Hilfeleistungen;
- Buchungsabschnitt 005: Ausgaben aufgrund Zuwendungen Dritter durch andere freiwillige Geldleistungen.

4.5.2 Leistungen öffentlich-rechtlicher Körperschaften

437. Die Feststellung, ob es sich bei einer Zuwendung um eine Leistung einer öffentlich-rechtlichen Körperschaft handelt, trifft grundsätzlich die Leitung der Dienststelle oder des Truppenteils, die oder der die Leistung erhalten soll.

438. Leistungen öffentlich-rechtlicher Körperschaften sind dem Referat R III 1 ES im BMVg vor ihrer Annahme auf dem Dienstweg zu melden und gemäß Nr. 436 zu buchen.

4.5.3 Fälle/Veranstaltungen mit gleichgerichteter Zielsetzung bei angemessener Kostenteilung (Kooperationen im Sinne der Verwaltungsvorschrift Sponsoring)

439. Die Feststellung, ob ein Fall der gleichgerichteten Zielsetzung bei angemessener Kostenteilung vorliegt, trifft das Referat R III 1 ES im BMVg.

440. Geplante Veranstaltungen mit einer möglichen gleichgerichteten Zielsetzung sind dem Referat R III 1 ES im BMVg mindestens acht Wochen vor ihrer Durchführung auf dem Dienstweg zu melden. Die Meldung hat bereits Angaben zu den ersten drei Punktaufzählungen der Nr. 441 zu enthalten.

441. In einer Kooperationsvereinbarung sollten – neben ggf. allgemeinen Vertragsbestandteilen – um die Abgrenzung zum Sponsoring klar zu definieren, mindestens folgende Punkte geregelt werden:

- Zweck und gemeinsames Ziel der Kooperation,
- Aufgabenverteilung und Pflichten der Kooperationspartner,
- Finanzierungs-/Kostenanteile (auch indirekt anfallende) und
- Dauer der Kooperation.

4.6 Jährlicher Bericht

442. Über alle Geld-, Sach- oder Dienstleistungen, deren Annahme nach den Nrn. 426, 427 und 428 zugestimmt wurde, ist dem Referat R III 1 ES im BMVg durch die annehmende Dienststelle/den annehmenden Truppenteil nach Aufforderung jährlich zum 31. Januar für das vergangene Jahr auf dem Dienstweg zu berichten.

B

443. Der Bericht muss mindestens die annehmende Dienststelle/den annehmenden Truppenteil, Namen, Wohnanschrift oder den Firmensitz des Zuwendungsgebers bzw. der Zuwendungsgeberin, die Art der Leistung (Geld-, Sach- oder Dienstleistung), deren Wert sowie die Gegenleistung der Dienststelle/des Truppenteils und den Verwendungszweck (bei Veranstaltungen auch: Ort und Datum) enthalten. Der Wert ist gegebenenfalls zu schätzen und getrennt nach Geld-, Sach- oder Dienstleistung aufzuführen.

5 Anlagen

5.1 Rundschreiben zum Verbot der Annahme von Belohnungen oder Geschenken in der Bundesverwaltung des BMI D I 3 – 210 170/1 vom 8. November 2004 (GMBl 2004, S. 1074) 22

5.2 Allgemeine Verwaltungsvorschrift zur Förderung von Tätigkeiten des Bundes durch Leistungen Privater (Sponsoring, Spenden und sonstige Schenkungen) vom 7. Juli 2003 22

5.3 Textbausteine für Ablehnungen von Belohnungen oder Geschenken 22

5.4 Bezugsjournal 23

5.5 Änderungsjournal 23

5.1 Rundschreiben zum Verbot der Annahme von Belohnungen oder Geschenken in der Bundesverwaltung des BMI D I 3 – 210 170/1 vom 8. November 2004 (GMBl 2004, S. 1074)

5.2 Allgemeine Verwaltungsvorschrift zur Förderung von Tätigkeiten des Bundes durch Leistungen Privater (Sponsoring, Spenden und sonstige Schenkungen) vom 7. Juli 2003

5.3 Textbausteine für Ablehnungen von Belohnungen oder Geschenken

Die **Anlagen 5.1 bis 5.3** stehen im Regelungsportal über die Registerkarte „Anhänge“ der Regelungsseite als Einzeldokumente zum Download bereit.

5.4 Bezugsjournal

(Nr.) Bezugsdokumente	Titel
1. Rdschr. BMI	Rundschreiben zum Verbot der Annahme von Belohnungen oder Geschenken in der Bundesverwaltung des BMI D I 3 – 210 170/1 vom 8. November 2004
2. VV Sponsoring	Allgemeine Verwaltungsvorschrift zur Förderung von Tätigkeiten des Bundes durch Leistungen Privater (Sponsoring, Spenden und sonstige Schenkungen) des BMI vom 7. Juli 2003
3. BBG	Bundesbeamtengesetz
4. SG	Soldatengesetz
5. TVöD	Tarifvertrag für den öffentlichen Dienst
6. BRKG	Bundesreisekostengesetz
7. SGB V	Sozialgesetzbuch V
8. IR BMVg Teil II	Interne Regelungen des BMVg Teil II
9. A-110/1 VS-NfD	Anerkennung von Verwendungen als Missionen

5.5 Änderungsjournal

Version	Gültig ab	Geänderter Inhalt
1	25.06.2020	• Erstveröffentlichung

Signatures

Number of pages (including this one): 24

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

Interimsfassung der Nrn. 11.4 und Nr. 11.5 der Zusätzlichen Vertragsbedingungen des Bundesministeriums der Verteidigung zur Verdingungsordnung für Leistungen Teil B (ZVB/BMVg) vom 28.01.2005

(Diese Regelung ist gültig bis zum Inkrafttreten einer Neufassung der ZVB/BMVg vom 28.01.1998 in der Fassung der 1. Änderung vom 10.05.2001)

11.4 Vertragsstrafe wegen Versprechens oder Gewährens von Vorteilen

11.4.1 Auftragnehmer oder ihre Beauftragten dürfen Personen, die beim Auftraggeber mit Aufgaben auf dem Gebiet der Forschung, Entwicklung oder Beschaffung betraut sind, weder unmittelbar noch mittelbar Vorteile im Sinne des § 331 des Strafgesetzbuches anbieten, versprechen oder gewähren.
Die vorgenannte Verpflichtung gilt für diesen Vertrag und für alle künftigen Geschäftsbeziehungen.

11.4.2 Handelt der Auftragnehmer der Verpflichtung nach Nr. 11.4.1 zuwider, hat er dem Auftraggeber eine Vertragsstrafe in Höhe von 5 v. H. der (nach der Zuwiderhandlung) vereinbarten Auftragssumme zu zahlen.
Kommt es nach einer Zuwiderhandlung zu Folgeverträgen, sind bei der Berechnung der Vertragsstrafe die Auftragssummen aus diesen Folgeverträgen innerhalb von 3 Jahren einzurechnen.
Die Höhe der Vertragsstrafe darf den 20-fachen Wert des Vorteils gemäß Nr. 11.4.1, insgesamt jedoch 500.000,-- Euro, nicht übersteigen. Eine im gleichen Zusammenhang verhängte kartellrechtliche Geldbuße wird auf die festgesetzte Vertragsstrafe angerechnet.
Die Geltendmachung eines Schadensersatzes durch den Auftraggeber infolge einer begangenen Verfehlung bleibt von der Vertragsstrafe unberührt, wobei in diesem Fall eine verwirkte Vertragsstrafe auf diesen Schadensersatz angerechnet wird.

Bei der Berechnung der Vertragsstrafe bleiben Aufträge außer Betracht, bei denen der Auftragnehmer nachweist, dass die Zuwiderhandlung gegen Nr. 11.4.1 nach allgemeiner Lebenserfahrung nicht geeignet war, die Entscheidung(en) in der amtsseitigen Auftragsbearbeitung unmittelbar oder mittelbar zu beeinflussen.
Ferner bleiben bei der Berechnung der Vertragsstrafe Aufträge, die nach Bekanntwerden der Zuwiderhandlung erteilt werden, außer Betracht.

11.5 Vertragsstrafe wegen Gewährens eines Tätigkeitsverhältnisses ohne Unbedenklichkeitsbestätigung

11.5.1 Auch das Gewähren eines Tätigkeitsverhältnisses, das arbeitsrechtlich bzw. dienstrechtlich als eine Nebentätigkeit oder eine Ruhestandstätigkeit zu bewerten ist, kann ein unzulässiger Vorteil i. S. von Nr. 11.4.1 sein. Daher verpflichtet sich der Auftragnehmer vor der Vereinbarung jeder Nebentätigkeit - einschließlich Gutachtertätigkeit - mit einem Bundeswehrangehörigen, sich von diesem eine Unbedenklichkeitsbestätigung des Auftraggebers (Bundesministerium der Verteidigung) vorlegen zu lassen.

Ferner verpflichtet sich der Auftragnehmer, einem Ruhestandsbeamten der Bundeswehr oder einem Berufssoldaten im Ruhestand, der nicht länger als fünf Jahre im Ruhestand ist, nur dann eine Tätigkeit zu übertragen, wenn ihm dieser hierfür eine Unbedenklichkeitsbestätigung des Auftraggebers (Bundesministerium der Verteidigung) vorgelegt hat. Bei Ruhestandsbeamten, die mit Vollendung des 65. Lebensjahres in den Ruhestand treten, beträgt die Frist drei Jahre. Ist die Tätigkeit in der Unbedenklichkeitsbestätigung unter Auflagen zugelassen worden, hat der Auftragnehmer die Auflagen zu beachten.

11.5.2 Der Auftragnehmer hat dem Auftraggeber, sofern die nach Nr. 11.5.1 erforderliche Unbedenklichkeitsbestätigung nicht erteilt wird, eine Vertragsstrafe in Höhe des Fünffachen des seit der Zuwiderhandlung gewährten Entgeltes, mindestens jedoch 5000,-- Euro und höchstens 100.000,-- Euro, zu zahlen.
Bei der Berechnung ist § 4 der Bundesnebentätigkeitsverordnung in der jeweils gültigen Fassung zugrunde zu legen. Es gilt der Bruttobetrag. Im Übrigen gelten die Regelungen nach Nr. 11.4 entsprechend.

11.5.3 Die Vertragsstrafe entfällt, wenn die Nebentätigkeit oder Ruhestandstätigkeit rechtmäßig ist bzw. nachträglich genehmigt wird.

11.5.4 Auf Verlangen des Auftraggebers wird der Auftragnehmer die für die Berechnung der Vertragsstrafe erforderlichen Auskünfte erteilen.

Signatures

Number of pages (including this one): 3

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

Niederschrift

über die förmliche Verpflichtung nichtbeamteter Personen

Ort, Datum

Verhandelt

Vor dem/der Unterzeichnenden erschien heute zum Zwecke der Verpflichtung nach § 1 des Gesetzes über die förmliche Verpflichtung nichtbeamteter Personen vom 2. März 1974 (BGBl I S. 469, 547).

Herr/Frau

Der/Die Erschienene wurde auf die gewissenhafte Erfüllung seiner/ihrer Obliegenschaften verpflichtet. Ihm/Ihr wurde der Inhalt der folgenden Strafvorschriften des Strafgesetzbuches bekannt gegeben:

§ 133 Abs. 3	- Verwahrungsbruch,
§ 201 Abs. 3	- Verletzung der Vertraulichkeit des Wortes,
§ 203 Abs. 2, 4, 5	- Verletzung von Privatgeheimnissen,
§ 204	- Verwertung fremder Geheimnisse,
§§ 331, 332	- Vorteilsannahme und Bestechlichkeit,
§ 353b	- Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht,
§ 358	- Nebenfolgen,
§ 97b Abs. 2 i.V.m. §§ 94 bis 97a	- Verrat in irriger Annahme eines illegalen Geheimnisses,
§ 120 Abs. 2	- Gefangenenbefreiung,
§ 355	- Verletzung des Steuergeheimnisses.

Der/Die Erschienene wurde darauf hingewiesen, dass die vorgenannten Strafvorschriften auf Grund der Verpflichtung für ihn/sie anzuwenden sind.

Er/Sie erklärt, nunmehr von dem Inhalt der genannten Bestimmungen unterrichtet zu sein. Er/Sie unterzeichnet dieses Protokoll nach Vorlesung zum Zeichen der Genehmigung und bestätigt gleichzeitig den Empfang einer Abschrift der Niederschrift und der oben genannten Vorschriften.

v.u.g.

Unterschrift des/der Verpflichtenden

Unterschrift des/der Verpflichteten

Strafvorschriften des Strafgesetzbuches

§ 133
Verwahrungsbruch

(1) Wer Schriftstücke oder andere bewegliche Sachen, die sich in dienstlicher Verwahrung befinden oder ihm oder einem anderen dienstlich in Verwahrung gegeben worden sind, zerstört, beschädigt, unbrauchbar macht oder der dienstlichen Verfügung entzieht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Dasselbe gilt für Schriftstücke oder andere bewegliche Sachen, die sich in amtlicher Verwahrung einer Kirche oder anderen Religionsgesellschaft des öffentlichen Rechts befinden oder von dieser dem Täter oder einem anderen amtlich in Verwahrung gegeben worden sind.

(3) Wer die Tat an einer Sache begeht, die ihm als Amtsträger oder für den öffentlichen Dienst besonders Verpflichteten anvertraut worden oder zugänglich geworden ist, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

§ 201
Verletzung der Vertraulichkeit des Wortes

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt

1. das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder
2. eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht.

(2) Ebenso wird bestraft, wer unbefugt

1. das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder
2. das nach Absatz 1 Nr. 1 aufgenommene oder nach Absatz 2 Nr. 1 abgehörte nichtöffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.

Die Tat nach Satz 1 Nr. 2 ist nur strafbar, wenn die öffentliche Mitteilung geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen. Sie ist nicht rechtswidrig, wenn die öffentliche Mitteilung zur Wahrnehmung überragender öffentlicher Interessen gemacht wird.

(3) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer als Amtsträger oder als für den öffentlichen Dienst besonders Verpflichteter die Vertraulichkeit des Wortes verletzt (Absätze 1 und 2).

(4) Der Versuch ist strafbar.

(5) Die Tonträger und Abhörgeräte, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden.

§ 203
Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,
3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,
4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist.

4a. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,

5. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,
4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,
5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder

6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist,

anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(2a) Die Absätze 1 und 2 gelten entsprechend, wenn ein Beauftragter für den Datenschutz unbefugt ein fremdes Geheimnis im Sinne dieser Vorschriften offenbart, das einem in den Absätzen 1 und 2 Genannten in dessen beruflicher Eigenschaft anvertraut worden oder sonst bekannt geworden ist und von dem er bei der Erfüllung seiner Aufgaben als Beauftragter für den Datenschutz Kenntnis erlangt hat.

(3) Einem in Absatz 1 Nr. 3 genannten Rechtsanwalt stehen andere Mitglieder einer Rechtsanwaltskammer gleich. Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Den in Absatz 1 und den in Satz 1 und 2 Genannten steht nach dem Tod des zur Wahrung des Geheimnisses Verpflichteten ferner gleich, wer das Geheimnis von dem Verstorbenen oder aus dessen Nachlass erlangt hat.

(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(5) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

§ 204
Verwertung fremder Geheimnisse

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach § 203 verpflichtet ist, verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 203 Abs. 4 gilt entsprechend.

§ 331 Vorteilsannahme

(1) Ein Amtsträger oder ein für den öffentlichen Dienst besonders Verpflichteter, der für die Dienstausübung einen Vorteil für sich oder einen Dritten fordert, sich versprechen läßt oder annimmt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Ein Richter oder Schiedsrichter, der einen Vorteil für sich oder einen Dritten als Gegenleistung dafür fordert, sich versprechen läßt oder annimmt, dass er eine richterliche Handlung vorgenommen hat oder künftig vornehme, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

(3) Die Tat ist nicht nach Absatz 1 strafbar, wenn der Täter einen nicht von ihm geforderten Vorteil sich versprechen läßt oder annimmt und die zuständige Behörde im Rahmen ihrer Befugnisse entweder die Annahme vorher genehmigt hat oder der Täter unverzüglich bei ihr Anzeige erstattet und sie die Annahme genehmigt.

§ 332
Bestechlichkeit

(1) Ein Amtsträger oder ein für den öffentlichen Dienst besonders Verpflichteter, der einen Vorteil für sich oder einen Dritten als Gegenleistung dafür fordert, sich versprechen lässt oder annimmt, dass er eine Diensthandlung vorgenommen hat oder künftig vornehme und dadurch seine Dienstpflichten verletzt hat oder verletzen würde, wird mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bestraft. In minder schweren Fällen ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe. Der Versuch ist strafbar.

(2) Ein Richter oder Schiedsrichter, der einen Vorteil für sich oder einen Dritten als Gegenleistung dafür fordert, sich versprechen läßt oder annimmt, dass er eine richterliche Handlung vorgenommen hat oder künftig vornehme und dadurch seine richterlichen Pflichten verletzt hat oder verletzen würde, wird mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren bestraft. In minder schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu fünf Jahren.

(3) Falls der Täter den Vorteil als Gegenleistung für eine künftige Handlung fordert, sich versprechen lässt oder annimmt, so sind die Absätze 1 und 2 schon dann anzuwenden, wenn er sich dem anderen gegenüber bereit gezeigt hat,
1. bei der Handlung seine Pflichten zu verletzen oder,
2. soweit die Handlung in seinem Ermessen steht, sich bei Ausübung des Ermessens durch den Vorteil beeinflussen zu lassen.

§ 353b
Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht

(1) Wer ein Geheimnis, das ihm als
1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten oder

3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,

anvertraut worden oder sonst bekanntgeworden ist, unbefugt offenbart und dadurch wichtige öffentliche Interessen gefährdet, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. Hat der Täter durch die Tat fahrlässig wichtige öffentliche Interessen gefährdet, so wird er mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Wer, abgesehen von den Fällen des Absatzes 1, unbefugt einen Gegenstand oder eine Nachricht, zu deren Geheimhaltung er

1. auf Grund des Beschlusses eines Gesetzgebungsorgans des Bundes oder eines Landes oder eines seiner Ausschüsse verpflichtet ist oder
2. von einer anderen amtlichen Stelle unter Hinweis auf die Strafbarkeit der Verletzung der Geheimhaltungspflicht förmlich verpflichtet worden ist,

an einen anderen gelangen lässt oder öffentlich bekanntmacht und dadurch wichtige öffentliche Interessen gefährdet, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(3) Der Versuch ist strafbar.

(3a) Beihilfehandlungen einer in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Person sind nicht rechtswidrig, wenn sie sich auf die Entgegennahme, Auswertung oder Veröffentlichung des Geheimnisses oder des Gegenstandes oder der Nachricht, zu deren Geheimhaltung eine besondere Verpflichtung besteht, beschränken.

(4) Die Tat wird nur mit Ermächtigung verfolgt. Die Ermächtigung wird erteilt

1. von dem Präsidenten des Gesetzgebungsorgans
   a) in den Fällen des Absatzes 1, wenn dem Täter das Geheimnis während seiner Tätigkeit bei einem oder für ein Gesetzgebungsorgan des Bundes oder eines Landes bekanntgeworden ist,
   b) in den Fällen des Absatzes 2 Nr. 1;
2. von der obersten Bundesbehörde
   a) in den Fällen des Absatzes 1, wenn dem Täter das Geheimnis während seiner Tätigkeit sonst bei einer oder für eine Behörde oder bei einer anderen amtlichen Stelle des Bundes oder für eine solche Stelle bekanntgeworden ist,
   b) in den Fällen des Absatzes 2 Nr. 2, wenn der Täter von einer amtlichen Stelle des Bundes verpflichtet worden ist;
3. von der obersten Landesbehörde in allen übrigen Fällen der Absätze 1 und 2 Nr. 2.

§ 358
Nebenfolgen

Neben einer Freiheitsstrafe von mindestens sechs Monaten wegen einer Straftat nach den §§ 332, 335, 339, 340, 343, 344, 345 Abs. 1 und 3, §§ 348, 352 bis 353b Abs. 1, §§ 355 und 357 kann das Gericht die Fähigkeit, öffentliche Ämter zu bekleiden (§ 45 Abs. 2), aberkennen.

§ 97b
Verrat in irriger Annahme eines illegalen Geheimnisses

(1) Handelt der Täter in den Fällen der §§ 94 bis 97 in der irrigen Annahme, das Staatsgeheimnis sei ein Geheimnis der in § 97a bezeichneten Art, so wird er, wenn

1. dieser Irrtum ihm vorzuwerfen ist,
2. er nicht in der Absicht handelt, dem vermeintlichen Verstoß entgegenzuwirken, oder
3. die Tat nach den Umständen kein angemessenes Mittel zu diesem Zweck ist,

nach den bezeichneten Vorschriften bestraft. Die Tat ist in der Regel kein angemessenes Mittel, wenn der Täter nicht zuvor ein Mitglied des Bundestages um Abhilfe angerufen hat.

(2) War dem Täter als Amtsträger oder als Soldat der Bundeswehr das Staatsgeheimnis dienstlich anvertraut oder zugänglich, so wird er auch dann bestraft, wenn nicht zuvor der Amtsträger einen Dienstvorgesetzten, der Soldat einen Disziplinarvorgesetzten um Abhilfe angerufen hat. Dies gilt für die für den öffentlichen Dienst besonders Verpflichteten und für Personen, die im Sinne des § 353b Abs. 2 verpflichtet worden sind, sinngemäß.

§ 94
Landesverrat

(1) Wer ein Staatsgeheimnis

1. einer fremden Macht oder einem ihrer Mittelsmänner mitteilt oder
2. sonst an einen Unbefugten gelangen lässt oder öffentlich bekanntmacht, um die Bundesrepublik Deutschland zu benachteiligen oder eine fremde Macht zu begünstigen,

und dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt, wird mit Freiheitsstrafe nicht unter einem Jahr bestraft.

(2) In besonders schweren Fällen ist die Strafe lebenslange Freiheitsstrafe oder Freiheitsstrafe nicht unter fünf Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. eine verantwortliche Stellung mißbraucht, die ihn zur Wahrung von Staatsgeheimnissen besonders verpflichtet, oder
2. durch die Tat die Gefahr eines besonders schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt.

§ 95
Offenbaren von Staatsgeheimnissen

(1) Wer ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird, an einen Unbefugten gelangen lässt oder öffentlich bekanntmacht und dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt, wird mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bestraft, wenn die Tat nicht in § 94 mit Strafe bedroht ist.

(2) Der Versuch ist strafbar.

(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren. § 94 Abs. 2 Satz 2 ist anzuwenden.

§ 96
Landesverräterische Ausspähung, Auskundschaften von Staatsgeheimnissen

(1) Wer sich ein Staatsgeheimnis verschafft, um es zu verraten (§ 94), wird mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren bestraft.

(2) Wer sich ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird, verschafft, um es zu offenbaren (§ 95), wird mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bestraft. Der Versuch ist strafbar.

§ 97
Preisgabe von Staatsgeheimnissen

(1) Wer ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird, an einen Unbefugten gelangen läßt oder öffentlich bekanntmacht und dadurch fahrlässig die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland verursacht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Wer ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird und das ihm kraft seines Amtes, seiner Dienststellung oder eines von einer amtlichen Stelle erteilten Auftrags zugänglich war, leichtfertig an einen Unbefugten gelangen läßt und dadurch fahrlässig die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland verursacht, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(3) Die Tat wird nur mit Ermächtigung der Bundesregierung verfolgt.

§ 97a
Verrat illegaler Geheimnisse

Wer ein Geheimnis, das wegen eines der in § 93 Abs. 2 bezeichneten Verstöße kein Staatsgeheimnis ist, einer fremden Macht oder einem ihrer Mittelsmänner mitteilt und dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt, wird wie ein Landesverräter (§ 94) bestraft. § 96 Abs. 1 in Verbindung mit § 94 Abs. 1 Nr. 1 ist auf Geheimnisse der in Satz 1 bezeichneten Art entsprechend anzuwenden.

§ 120
Gefangenenbefreiung

(1) Wer einen Gefangenen befreit, ihn zum Entweichen verleitet oder dabei fördert, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Ist der Täter als Amtsträger oder als für den öffentlichen Dienst besonders Verpflichteter gehalten, das Entweichen des Gefangenen zu verhindern, so ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) Einem Gefangenen im Sinne der Absätze 1 und 2 steht gleich, wer sonst auf behördliche Anordnung in einer Anstalt verwahrt wird.

§ 355
Verletzung des Steuergeheimnisses

(1) Wer unbefugt
1. Verhältnisse eines anderen, die ihm als Amtsträger
   a) in einem Verwaltungsverfahren oder einem gerichtlichen Verfahren in Steuersachen,
   b) in einem Strafverfahren wegen einer Steuerstraftat oder in einem Bußgeldverfahren wegen einer Steuerordnungswidrigkeit,
   c) aus anderem Anlass durch Mitteilung einer Finanzbehörde oder durch die gesetzlich vorgeschriebene Vorlage eines Steuerbescheids oder einer Bescheinigung über die bei der Besteuerung getroffenen Feststellungen bekanntgeworden sind, oder
2. ein fremdes Betriebs- oder Geschäftsgeheimnis, das ihm als Amtsträger in einem der in Nummer 1 genannten Verfahren bekanntgeworden ist,

offenbart oder verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Den Amtsträgern im Sinne des Absatzes 1 stehen gleich
1. die für den öffentlichen Dienst besonders Verpflichteten,
2. amtlich zugezogene Sachverständige und

3. die Träger von Ämtern der Kirchen und anderen Religionsgesellschaften des öffentlichen Rechts.

(3) Die Tat wird nur auf Antrag des Dienstvorgesetzten oder des Verletzten verfolgt. Bei Taten amtlich zugezogener Sachverständiger ist der Leiter der Behörde, deren Verfahren betroffen ist, neben dem Verletzten antragsberechtigt.

Signatures

Number of pages (including this one): 7

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.

BWI
IT für Deutschland

Open Source Software

Anlage 14 zum Rahmenvertrag über den Bezug von Konzeptions- und Entwicklungsleistungen für die „Strategische Partnerschaft pCloudBw“

☐ Option 1

Der Auftragnehmer erklärt, ausschließlich die im Anhang[1] zu dieser Anlage 14 aufgeführte Open Source Software im Rahmen der Leistungserbringung für den Auftraggeber unter Berücksichtigung der Regelungen des Rahmenvertrages zu Open Source Software einzusetzen.

Sofern sich Änderungen in Bezug auf eingesetzte Open Source Software ergeben, wird der Auftragnehmer den Auftraggeber hierüber unverzüglich schriftlich informieren und unverzüglich eine aktualisierte Fassung des Anhangs zur dieser Anlage 14 zur Verfügung stellen.

☒ Option 2

Der Auftragnehmer erklärt keine Open Source Software im Rahmen seiner Leistungserbringung einzusetzen.

[1] Vom Auftragnehmer auf Basis der Regelungen des Rahmenvertrages zu Open Source Software bereitzustellen.

Signatures

Number of pages (including this one): 3

- ✓ Document signed electronically, the signatories agreeing that it is authentic between them.
- ✓ By signing this document, the signatories acknowledge and agree that they have carefully read this document and approve all its terms.