Verpflichtungserklärung zur Einhaltung von Sicherheitsanforderungen

[Auftragnehmer], [Anschrift]

nachfolgend „Bieter / Auftragnehmer“

§ 1 Gegenstand des Auftrags

Erneuerung Redaktionsarbeitsplätze nur Fernwartung

§ 2 Anerkennung von Sicherheitsanforderungen*

Der Bieter / Auftragnehmer verpflichtet sich, die Sicherheitsanforderungen der nachfolgend als relevant markierten Kapitel des Dokuments „Sicherheitsanforderungen bei Ausschreibung“ vollumfänglich und verbindlich durch geeignete technische und organisatorische Maßnahmen (TOM) über den gesamten Zeitraum der Leistungserbringung zu erfüllen.

Relevante Kapitel:

- ☒ Kapitel 1: Sicherheitsanforderungen an IT-gestützte Dienstleistung
- ☐ Kapitel 2: Sicherheitsanforderungen bei Softwareentwicklung
- ☐ Kapitel 3: Sicherheitsanforderungen an Webanwendungen
- ☐ Kapitel 4: Sicherheitsanforderungen an Webserver
- ☐ Kapitel 5: Sicherheitsanforderungen an KI-Entwicklung und KI-Integration

§ 3 weitere Verpflichtungen

Der Bieter / Auftragnehmer verpflichtet sich:

- auf Anfrage sämtliche Informationen und Dokumentationen zum Nachweis der Konformität zur Verfügung zu stellen.
- dem Auftraggeber oder beauftragten Dritten in begründeten Fällen Zugang für eine Vor-Ort-Inspektion zu gewähren, z.B. im Zusammenhang mit möglichen Sicherheitsvorfällen. Der Auftraggeber teilt dem Bieter / Auftragnehmer in diesen Fällen rechtzeitig (in der Regel vier Wochen vorher) den Termin der Überprüfung mit. Außerordentliche oder behördlich verfügte Überprüfungen sind hiervon ausgenommen.
- bei Sicherheitsvorfällen oder festgestellten Sicherheitsrisiken unverzüglich Korrekturmaßnahmen zu ergreifen und den Auftraggeber zu informieren.
- im Falle der Einbindung von Subunternehmen, dafür zu sorgen, dass die hier genannten Sicherheitsanforderungen auch von diesen erfüllt und kontinuierlich überprüft werden.

Ort, Datum

Unterschrift
Bieter /Auftragnehmer

* von Auftraggeber auszufüllen

Sicherheitsanforderungen bei Ausschreibung

Hinweis:
Zur Vereinfachung der Lesbarkeit wird auf den folgenden Seiten die männliche Schreibweise verwendet.
Das Dokument gilt für alle Geschlechter.

Dokumenteninformation

Klassifikation:	Öffentlich		
Versionsnummer:	1.3		
Dokumententitel:	Sicherheitsanforderungen bei Ausschreibung		
Dokumentennummer:	ISB-SA-01Fehler! Unbekannter Name für Dokument-Eigenschaft.		
Verantwortlicher:	rbb Informationssicherheitsbeauftragter		
Erstellt am:	10.03.2022	Erstellt von:	Marcel Kuring
Nächste Überarbeitung:	02/2028	Überarbeitung durch:	Informationssicherheit
Status:	Freigegeben	Letzte Bearbeitung:	24.06.2026
Freigabe am:	24.06.2026	Freigabe von:	Informationssicherheit

Dokumentenverteiler

Berechtigte Rolle (Verteilerkreis)
Administratoren, Systemverantwortliche, Projektplaner, Bieter / Auftragnehmer

Versionsverlauf

Datum	Version	Beschreibung	verändert durch
10.03.2022	0.9	finaler Entwurf	Marcel Kuring
22.09.2022	1.0	Freigabe durch Informationssicherheitskreis	Marcel Kuring
15.01.2026	1.1	Erweiterung Anforderungen um IT-gestützte Dienstleistung	Marcel Kuring
19.03.2026	1.2	Anpassung in Anforderung IT-A12	Marcel Kuring
24.06.2026	1.3	Erweiterung Anforderungen um KI	Marcel Kuring

Ergänzende Dokumente / Mitgeltende Unterlagen [2]

Dokumentennummer	Titel	Verantwortlicher
BSI TR-02102	Kryptographische Verfahren: Empfehlungen und Schlüssellängen	BSI
EU 2024/1689	EU KI Verordnung	EU

[2] In der Tabelle sind alle Dokumente einzutragen, die für dieses Dokument Gültigkeit besitzen, die aber im Dokument nicht explizit genannt werden. Einzutragen sind auch alle Dokumente, auf die im nachfolgenden Dokument explizit verwiesen wird.

Inhalt

Kapitel 1: Sicherheitsanforderungen an IT-gestützte Dienstleistung 1
IT-A1 ISMS 1
IT-A2 Zutrittskontrolle 1
IT-A3 Härtung 1
IT-A4 Schwachstellen- und Patchmanagement 2
IT-A5 Schutz vor Cyberangriffen 2
IT-A6 Netzinfrastruktur 2
IT-A7 Verschlüsselung 2
IT-A8 Test + Freigabe 2
IT-A9 Mandantentrennung 3
IT-A10 Datensicherung und Wiederherstellung 3
IT-A11 Löschung 3
IT-A12 Identitäts- und Berechtigungsverwaltung 3
IT-A13 Authentisierung 3
IT-A14 Protokollierung 4
IT-A15 Exportierbarkeit / Portabilität 4
IT-A16 Sicherheitsvorfall 5
IT-A17 Subunternehmen 5
IT-A18 Datenschutz 5
IT-A19 Lokation + Gerichtsstand 6
IT-A20 Rechte 6
IT-A21 Unterweisung 6

Kapitel 2: Sicherheitsanforderungen bei Softwareentwicklung 7
SE-A1 Sicheres Systemdesign 7
SE-A2 Authentisierung 7
SE-A3 Protokollierung sicherheitsrelevanter Ereignisse 7
SE-A4 Verwendung von externen Bibliotheken aus vertrauenswürdigen Quellen 8
SE-A5 Durchführung von entwicklungsbegleitenden Software-Tests 8
SE-A6 Bereitstellung von Patches, Updates und Änderungen 8
SE-A7 Versionsverwaltung des Quellcodes 8
SE-A8 Überprüfung von externen Komponenten 9

Kapitel 3: Sicherheitsanforderungen an Webanwendungen 10
WA-A1 Authentisierung bei Webanwendungen 10
WA-A2 Protokollierung sicherheitsrelevanter Ereignisse von Webanwendungen 10
WA-A3 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates 10
WA-A4 Sichere Konfiguration der Webanwendung 10
WA-A5 Zugriffskontrolle bei Webanwendungen 10
WA-A6 Sicheres Session-Management 10
WA-A7 Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen 11
WA-A8 Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen 11
WA-A9 Schutz vor Standardbedrohungen 11
WA-A10 Schutz vertraulicher Daten 12
WA-A11 Umfassende Eingabevalidierung und Ausgabekodierung 12

Kapitel 4: Sicherheitsanforderungen an Webserver 13
WS-A1 Authentisierung bei Webservern 13
WS-A2 Protokollierung sicherheitsrelevanter Ereignisse von Webservern 13

WS-A3 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates 13
WS-A4 Sichere Konfiguration eines Webservers 13
WS-A5 Schutz der Webserver-Dateien 13
WS-A6 Absicherung von Datei-Uploads und -Downloads 13
WS-A7 Verschlüsselung über TLS 13
WS-A8 Schutz vor Denial-of-Service-Angriffen 14

Kapitel 5: Sicherheitsanforderung an KI-Entwicklung und KI-Integration 15
KI-A1 Betriebsdokumentation 15
KI-A2 Interventionsmöglichkeit 15
KI-A3 Sicherung des Versionsverlauf der KI-Lösung 15
KI-A4 Schutz von Test- und Trainingsdaten 15
KI-A5 Vorauswahl von Trainingsdaten 15
KI-A6 Trennung von Trainings- / Finetuning- und Nutzungsphase des KI-Modells 15
KI-A7 Ausgabeformate definieren und validieren 15
KI-A8 Metadatenverarbeitung von Quelldaten 15
KI-A9 Festlegung von Performanz-Metriken 16
KI-A10 Monitoring der Performanz-Metriken 16
KI-A11 Einhaltung von Berechtigungen 16
KI-A12 Rollen- Berechtigungsfunktion bei Grounding 16
KI-A13 Filterung der Eingabedaten 16
KI-A14 Dokumentation von Datenflüssen und Schnittstellen 16
KI-A15 Absicherung von Schnittstellen 16
KI-A16 Sperrung von Schnittstellen 16
KI-A17 Kennzeichnung von KI-Ausgaben 17
KI-A18 automatisierte Weiternutzung von KI-Ausgaben 17
KI-A19 Validierung der KI-Ausgabe 17
KI-A20 KI spezifische Penetrationstests 17

Kapitel 1: Sicherheitsanforderungen an IT-gestützte Dienstleistung

IT-gestützte Dienstleistung liegt vor, wenn IT-Systeme zur Erfüllung der beauftragten Dienstleistung eingesetzt werden. Beispiele sind: Support / Wartung, Penetrationstests, Bereitstellung und Verwaltung von Cloud-Diensten, Softwareentwicklung, Web-Hosting.

*Handelt es sich bei der IT-gestützten Dienstleistung um Fernwartung sind nur die mit * gekennzeichneten Anforderungen zu erfüllen.*

IT-A1 ISMS

1) Zertifizierung von Rechenzentren
   Alle beteiligten Rechenzentren, MÜSSEN im Rahmen eines Information Security Management System (ISMS) betrieben werden, welches nach ISO/IEC 27001, BSI IT-Grundschutz oder einem vergleichbaren, anerkannten Standard zertifiziert ist. Eine gültige Zertifizierung für das ISMS MUSS vor Beauftragung nachgewiesen werden.
2) Fortführung der Zertifizierung gewährleisten und nachweisen
   Bei Ablauf der Zertifizierung während der Beauftragung MUSS der Dienstleister die Fortführung der entsprechenden Zertifizierung gewährleisten und nachweisen.
3) Bei hohem Schutzbedarf
   Zertifizierung der Dienstleister bei hohem Schutzbedarf
   Alle an der beauftragten Dienstleistung beteiligten Dienstleister MÜSSEN ein Information Security Management System (ISMS) nach ISO/IEC 27001, BSI IT-Grundschutz oder einem vergleichbaren, anerkannten Standard betreiben. Die Information Security Management Systeme SOLLTEN zertifiziert sein und eine gültige Zertifizierung vor Beauftragung nachgewiesen werden.

IT-A2 Zutrittskontrolle

1) Umsetzung eines wirksamen Zutrittsschutzes
   Räumlichkeiten in denen Daten des Auftraggebers verarbeitet und gespeichert oder abgelegt werden, MÜSSEN gegen den Zutritt unbefugter Personen durch geeignete Maßnahmen abgesichert werden.
2) Festlegung zutrittsberechtigter Personen
   Der Kreis der zutrittsberechtigten Personen MUSS festgelegt werden und die Zutrittsberechtigungen zu Räumlichkeiten in denen Daten des Auftraggebers verarbeitet und gespeichert oder abgelegt werden, MÜSSEN auf das notwendige Minimum beschränkt werden.
3) Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen
   Beantragung, Genehmigung, Ausgabe, Verwaltung und Rücknahme von Zutrittsmitteln bzw. Entzug von Zutrittsrechten MÜSSEN personengebunden dokumentiert werden. Dies gilt auch für Besucher, Fremdpersonal, Reinigungs- und Wartungspersonal.

IT-A3 Härtung

1) Härtung der Front- und Backendsysteme*
   Die für die Erbringung der Dienstleistung genutzten Systeme MÜSSEN gehärtet sein. Hierzu zählen u.a. die Deinstallation nicht notwendiger Software-Pakete; Deaktivierung/Abschaltung von nicht benötigten Programmen, Diensten, Konten, Services

und Ports; die Anpassung von Konfigurationen; das Erzwingen von Firewall-Regeln; Änderung von Standardpasswörtern.

IT-A4 Schwachstellen- und Patchmanagement

1) Betrieb eines Schwachstellen- und Patchmanagements
   Der Dienstleister MUSS ein Verfahren für seine Verarbeitungsanlagen betreiben, das Schwachstellen erkennt, bewertet, priorisiert und zeitnah behebt. z.B. Patchmanagement, regelmäßige Penetrationstests

IT-A5 Schutz vor Cyberangriffen

1) Erkennung und Abwehr von Cyberangriffen*
   Es MUSS ein geeigneter und aktueller Schutz vor Cyberangriffen nach dem aktuellen Stand der Technik eingerichtet sein. z.B. End-Point-Protection, Einbruchserkennungssysteme (IDS/IPS), zentrale Logauswertung (SIEM), Security Operation Center (SOC), Computer Emergency Response Team (CERT).

IT-A6 Netzinfrastruktur

1) Implementation von Sicherheitsgateways*
   Zur Abwehr netzbasierter Angriffe MÜSSEN wirksame Sicherheitsmaßnahmen (d.h. Firewalls, Netzwerksegmentierung, unterschiedliche Sicherheitszonen) nach dem aktuellen Stand der Technik etabliert sein.

IT-A7 Verschlüsselung

1) Verschlüsselung nach Stand der Technik*
   Der Dienstleister MUSS sich bei Verwendung von Verschlüsselungsverfahren nach dem aktuellen Stand der Technik (beispielsweise siehe BSI TR-02102[3]) richten.
2) Verschlüsselte Datenübertragung zu externen Systemen*
   Transport: Jegliche Datenkommunikation MUSS auf dem Transportweg verschlüsselt werden.
3) Verschlüsselung ruhender Daten*
   Der Dienstleister MUSS die ruhenden Daten auf Datenträgern verschlüsselt speichern. Dabei MUSS ein Verfahren genutzt werden, dass dem aktuellen Stand der Technik entspricht.

IT-A8 Test + Freigabe

1) Prozess für Test und Freigabe
   Es MUSS ein geeigneter Prozess für Tests und Freigabe für alle Komponenten der Dienstleistung etabliert sein.
2) Test neuer Hard und Software*
   Es MUSS sichergestellt werden, dass der produktive Einsatz von Komponenten erst nach erfolgreichem Test und Freigabe erfolgt.
3) Trennung von Produktiv-, Test und Entwicklungsumgebungen*
   Entwicklungs-, Test- und Produktivumgebung SOLLTEN getrennt sein.

[3] Aktuelle Technische Richtlinie beim BSI: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

IT-A9 Mandantentrennung

1) Trennung von Mandanten
   Es MUSS eine wirksame Mandantentrennung gewährleistet sein. Die Daten des Auftraggebers MÜSSEN dabei logisch von denen anderer Kunden getrennt sein.

IT-A10 Datensicherung und Wiederherstellung

1) Durchführung von Datensicherungen
   Der Dienstleister SOLLTE Verfahren zu Datensicherung und Wiederherstellung nach dem aktuellen Stand der Technik anbieten.
2) Umsetzung eines Datensicherungskonzeptes
   Die Vorgaben des Auftraggebers zu Aufbewahrungszeiten und Wiederherstellungszeiten MÜSSEN umgesetzt werden können.
3) Bei hohem Schutzbedarf der Verfügbarkeit
   Durchführung von Datensicherung bei hohem Schutzbedarf
   Bei hohem Schutzbedarf der Verfügbarkeit MUSS der Dienstleister Verfahren zu Datensicherung und Wiederherstellung nach dem aktuellen Stand der Technik anbieten.

IT-A11 Löschung

1) Löschung und Entsorgung nach dem Stand der Technik*
   Nicht mehr benötigte Daten und Informationen MÜSSEN nach dem aktuellen Stand der Technik vernichtet bzw. gelöscht werden. Nach Beendigung der Beauftragung MÜSSEN alle Daten und Informationen des Auftraggebers unwiederbringlich gelöscht werden. Dem Auftraggeber darf kein Schaden durch nicht vernichtete bzw. gelöschte Daten und Informationen entstehen.
2) Bei hohem Schutzbedarf der Vertraulichkeit
   Nachweis der Datenlöschung
   Als Nachweis SOLLTE dem Auftraggeber ein Löschprotokoll bzw. ein Löschbericht vorgelegt werden, der diesen Datenlöschprozess belegen kann.

IT-A12 Identitäts- und Berechtigungsverwaltung

1) Dokumentierte Verwaltung von Identitäten und Berechtigungen
   Es MUSS eine dokumentierte und stets aktuelle Identitäts- und Berechtigungsverwaltung existieren, die mindestens eine Trennung zwischen Benutzer und administrativen Konten (schließt auch Konten des Dienstleisters ein) ermöglicht.
2) Umsetzung des Need-to-known-Prinzips*
   Es MUSS gewährleistet werden, dass alle Benutzer und Administratoren nur diejenigen Berechtigungen besitzen, die zur Erfüllung der jeweiligen Aufgaben erforderlich sind (Prinzip der minimalen Rechte bzw. least privilege) und bei personellen Veränderungen (z.B. Funktionswechsel, Ausscheiden) Berechtigungen entzogen werden.

IT-A13 Authentisierung

1) Authentifizierung nach dem Stand der Technik*
   Der Zugang zu Informationen und Systemen MUSS durch eine sichere Authentisierung nach dem aktuellen Stand der Technik geschützt werden. Dies gilt auch für alle Fernzugänge und Schnittstellen.
2) Zugang aus ungeschützten Netzen*

Grundsätzlich MUSS immer eine Multi-Faktor-Authentisierung verwendet werden. Kann eine Multi-Faktor-Authentisierung nicht umgesetzt werden, darf der Zugang auf den Dienst ausschließlich auf vom Auftraggeber benannten IP-Adressbereichen (z.B. Datennetz der Rundfunkanstalt) erfolgen.

3) Starke Authentisierung bei privilegierten Zugängen*
   Für privilegierte Zugänge (administrative Zugänge) MUSS eine Multi-Faktor-Authentisierung verwendet werden. Dies gilt auch für alle Fernzugänge und Schnittstellen.
4) Einfache Authentifizierung (per Benutzername/Passwort) bei normalem Schutzbedarf*
   Bei Verwendung von Passwörtern:
   Es MUSS technisch sichergestellt werden, dass ausschließlich komplexe Passwörter verwendet werden (3 aus den folgenden 4 Merkmalen: Großbuchstabe, Kleinbuchstabe, Ziffer, Sonderzeichen; Einhaltung einer definierten Mindestlänge von 10 Zeichen).
5) Umsetzung von Vorgaben einer Passwortrichtlinie
   Die Vorgaben einer Passwortrichtlinie MÜSSEN umgesetzt werden können (Definition von Passworthistorie, Passwortalter, Passwortlänge).
6) Gesicherte Übertragung von Authentisierungsinformationen im Netzwerk
   Übertragung der Authentisierungsinformationen (z.B. Passwörter, Pin, biometrische Merkmale):
   Die Übertragung der Authentisierungsgeheimnissen MUSS mit einem sicheren Verschlüsselungsverfahren nach aktuellem Stand der Technik (beispielsweise siehe BSI TR-02102) abgesichert werden.
7) Speicherung von Authentisierungsinformationen*
   Authentifizierungsinformationen MÜSSEN nach dem aktuellen Stand der Technik geschützt werden (z.B. TPM, sichere Hash-Verfahren wie Argon2).
8) Änderung voreingestellter Authentisierungsinformationen
   Voreingestellte Authentisierungsinformationen (z.B. Initialkennungen und Passwörter) MÜSSEN geändert werden können.

IT-A14 Protokollierung

1) Protokollierung sicherheitsrelevanter Ereignisse
   Sicherheitsrelevante Ereignisse (z.B. erfolgreiche Zugriffe auf Ressourcen, fehlgeschlagene Zugriffe auf Ressourcen aufgrund von mangelnder Berechtigung, nicht vorhandenen Ressourcen und Fehlern, allgemeine Fehlermeldungen, Löschen) MÜSSEN in der Art protokolliert werden, dass sie im Nachgang ausgewertet werden können.
2) Sicherung der Protokolldaten vor Verlust und Veränderung
   Protokollierungsdaten MÜSSEN vor unberechtigtem Zugriff und Manipulation geschützt werden.
3) Kontrolle der Protokolldaten
   Der Dienstleister MUSS die Protokolle regelmäßig auswerten. Unregelmäßigkeiten MÜSSEN dokumentiert und dem Auftraggeber unverzüglich gemeldet werden.

IT-A15 Exportierbarkeit / Portabilität

1) Portabilität bei Vertragsende
   Bei Vertragsende MÜSSEN die Daten des Auftraggebers in elektronischen Standardformaten, wie z. B. CSV, XML, ZIP-Archiv portierbar und exportierbar sein.
2) Bei hohem Schutzbedarf der Verfügbarkeit:
   Portabilität bei hohem Schutzbedarf

Eine Übertragung bzw. Rückführung der Daten MUSS möglich sein. Dazu MÜSSEN durch den Dienstleister entsprechende Schnittstellen, wie z.B. API, Protokolle bereitgestellt werden.

IT-A16 Sicherheitsvorfall

1) Incident-Response-Management
   Der Auftraggeber MUSS über alle ihn betreffende Sicherheitsvorfälle und deren mögliche Auswirkungen unverzüglich und in geeigneter Weise informiert werden. Dafür MÜSSEN Ansprechpartner beim Auftraggeber und beim Dienstleister benannt werden.
2) Notfallvorsorge
   Zur Schadensminimierung und weiterer Schadensabwehr MUSS der Dienstleister geeignete Verfahren zur Notfallvorsorge z.B. BCM etabliert haben.
3) Angriffserkennung und -abwehr
   Es MÜSSEN Methoden und Technologien verwendet werden, um Cyberangriffe auf die Dienstleistung (z.B. DDoS, Brute-Force) zu erkennen und abzuwehren.

IT-A17 Subunternehmen

1) Verpflichtung von Subunternehmen*
   Der Dienstleister MUSS dafür sorgen, dass bei Involvierung von Subunternehmen die vom Auftraggeber gestellten Sicherheitsanforderungen auch von Subunternehmen erfüllt werden. Dies MUSS durch den Dienstleister kontinuierlich überprüft werden.
2) Benennung von Subunternehmen*
   Der Dienstleister MUSS alle Subunternehmen vollständig benennen. Dabei MUSS ersichtlich sein auf welche Art und in welchem Umfang Subunternehmen in die Bereitstellung der Dienstleistung einbezogen werden.
3) Bei hohem Schutzbedarf
   Meldung von Änderungen bei Subunternehmen*
   Beabsichtigte Änderungen an vertraglichen Vereinbarungen mit Subunternehmen, die in die Bereitstellung der Dienstleistung involviert sind, MÜSSEN dem Auftraggeber unverzüglich, vor Umsetzung der Änderung, schriftlich oder per E-Mail mitgeteilt werden.

IT-A18 Datenschutz

1) Umsetzung von Anonymisierung
   Sofern vom Auftraggeber gefordert MÜSSEN Maßnahmen zur Anonymisierung, die eine Zuordnung bzw. Verbindung zu einer Person unmöglich machen (z.B. durch Informationsreduktion, datenveränderte Verfahren, Mikroaggregationsverfahren) umgesetzt werden.
2) Umsetzung von Pseudonymisierung
   Sofern vom Auftraggeber gefordert MÜSSEN Maßnahmen zur Pseudonymisierung (z.B. Transformationsverfahren) nach Stand der Technik (z.B. aktuelle BSI-Richtlinien zu Kryptoverfahren) umgesetzt werden.
3) getrennte Verarbeitung*
   Der Auftragsverarbeiter stellt sicher, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden. Die Trennung der Daten wird so gestaltet, dass eine Vermischung von Daten für unterschiedliche Verarbeitungszwecke nicht möglich ist (z.B. physikalische bzw. logische Trennung von Systemen, Datenbanken und Datenträgern, Steuerung über Berechtigungskonzepte).
4) Protokollierung bei Lese-, Eingabe-, Änderungs- und Löschtransaktionen

Alle Lese-, Eingabe-, Änderungs- und Löschtransaktionen von personenbezogenen Daten MÜSSEN protokolliert werden.

IT-A19 Lokation + Gerichtsstand

1) Angaben zur Gerichtsbarkeit
   Der Dienstleister MUSS nachvollziehbare und transparente Angaben zu seiner Gerichtsbarkeit sowie der Lokation der Daten bei Datenspeicherung, -verarbeitung und -sicherung machen.
2) Verarbeitung im Europäischen Wirtschaftsraum
   Die Daten und Informationen SOLLTEN innerhalb des Europäischen Wirtschaftsraums (EWR) verarbeitet bzw. gespeichert werden.
3) Bei hohem Schutzbedarf für Vertraulichkeit oder Integrität
   Festlegung der Lokation bei hohem Schutzbedarf
   Der Auftraggeber MUSS in der Lage sein, die Lokationen (Ort/Land) der Datenspeicherung, -verarbeitung und -sicherung festzulegen.

IT-A20 Rechte

1) Klärung von Urheber-, Nutzungs- oder Verwertungsrechten
   Der Auftraggeber MUSS alle Urheber-, Nutzungs- oder Verwertungsrechte an den Daten und Informationen, die im Rahmen der Beauftragung gespeichert, verarbeitet oder gesichert werden behalten.

IT-A21 Unterweisung

1) Unterweisung in Datenschutz und Informationssicherheit*
   Alle an der Erbringung der Dienstleistung beteiligten Personen MÜSSEN regelmäßig hinsichtlich der Datenschutz- und Informationssicherheitsvorschriften unterwiesen werden.

Kapitel 2: Sicherheitsanforderungen bei Softwareentwicklung

SE-A1 Sicheres Systemdesign

1) Grundsätzlich MÜSSEN alle Eingabedaten vor der Weiterverarbeitung geprüft und validiert werden.
2) Bei Client-Server-Anwendungen MÜSSEN die Daten grundsätzlich auf dem Server validiert werden.
3) Die Standardeinstellungen der Software MÜSSEN derart voreingestellt sein, dass ein sicherer Betrieb der Software ermöglicht wird.
4) Es MUSS verhindert werden, dass bei Fehlern oder Ausfällen von Komponenten des Systems schützenswerte Informationen preisgegeben werden.
5) Die Software MUSS mit möglichst geringen Privilegien ausgeführt werden können.
6) Schützenswerte Daten MÜSSEN mit einer Methode, die dem aktuellen Stand der Technik entspricht, verschlüsselt übertragen und gespeichert werden. Die Empfehlungen der Technischen Richtlinie TR-02102[4] des BSI MÜSSEN beachtet werden.

SE-A2 Authentisierung

1) Es MUSS sichergestellt werden, dass sich Benutzer geeignet authentisieren, wenn diese auf geschützte Ressourcen zugreifen wollen. Dafür MUSS eine geeignete vertrauenswürdige Authentisierungsmethode ausgewählt werden (z.B. Anbindung an Microsoft AD / Azure AD).
2) Authentisierungsinformationen MÜSSEN verschlüsselt gespeichert oder übertragen werden. Die Empfehlungen der Technischen Richtlinie TR-02102 des BSI MÜSSEN beachtet werden.
3) Bei Nutzung von Passwörtern MÜSSEN Benutzer dazu gezwungen werden, sichere Passwörter zu benutzen (3 aus den folgenden 4 Merkmalen: Großbuchstabe, Kleinbuchstabe, Ziffer, Sonderzeichen; Einhaltung einer definierten Mindestlänge) und die Vorgaben einer Passwortrichtlinie MÜSSEN umgesetzt werden können (Definition von Passworthistorie, Passwortalter, Passwortlänge).
4) Zugänge auf geschützte Ressourcen, die aus dem Internet erreichbar sind, MÜSSEN mit einer Multi-Faktor-Authentisierung geschützt werden.
5) Sollen Authentisierungsdaten auf einem Client gespeichert werden, MUSS der Benutzer explizit zustimmen („Opt-In“).
6) Es MUSS einen Schutz vor Brute-Force-Angriffen geben.
7) Alle angebotenen Authentisierungsverfahren MÜSSEN das gleiche Sicherheitsniveau aufweisen.
8) In der Standardeinstellung MÜSSEN Authentisierungsinformationen bei der Eingabe ausgeblendet werden.
9) Voreingestellte Authentisierungsinformationen (z. B. Standard- oder Initialkennungen und Passwörter des Herstellers / Entwicklers) MÜSSEN noch vor der Inbetriebnahme in den Produktivbetrieb geändert werden.

SE-A3 Protokollierung sicherheitsrelevanter Ereignisse

1) Sicherheitsrelevante Ereignisse MÜSSEN in der Art protokolliert werden, dass sie im Nachgang ausgewertet werden können.

[4] Aktuelle Technische Richtlinie beim BSI: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

2) Bei automatisierter Auswertung der Protokollierungsdaten MUSS sichergestellt werden, dass Schadcode in Protokoll-Einträgen vom Auswertungsprogramm nicht interpretiert werden.
3) Der Zugriff auf Protokollierungsdaten MUSS auf einen definierten Personenkreis beschränkt werden können.
4) Es MÜSSEN mindestens folgende Ereignisse protokolliert werden:
   - erfolgreiche Zugriffe auf Ressourcen
   - fehlgeschlagene Zugriffe auf Ressourcen aufgrund von mangelnder Berechtigung, nicht vorhandenen Ressourcen und Fehlern
   - allgemeine Fehlermeldungen

SE-A4 Verwendung von externen Bibliotheken aus vertrauenswürdigen Quellen

1) Wird im Rahmen des Entwicklungs- und Implementierungsprozesses auf externe Bibliotheken zurückgegriffen, MÜSSEN diese aus vertrauenswürdigen Quellen bezogen werden.
2) Bevor externe Bibliotheken verwendet werden, MUSS deren Integrität sichergestellt werden.

SE-A5 Durchführung von entwicklungsbegleitenden Software-Tests

1) Schon bevor die Software im Freigabeprozess getestet und freigegeben wird, MÜSSEN entwicklungsbegleitende Software-Tests durchgeführt und der Quellcode auf Fehler gesichtet werden.
2) Die entwicklungsbegleitenden Tests MÜSSEN die funktionalen und nichtfunktionalen Anforderungen der Software umfassen. Die Software-Tests MÜSSEN dabei auch Negativtests abdecken. Zusätzlich MÜSSEN auch alle kritischen Grenzwerte der Eingabe sowie der Datentypen überprüft werden.
3) Die Software MUSS in einer Test- und Entwicklungsumgebung getestet werden, die getrennt von der Produktionsumgebung ist.
4) Es MUSS getestet werden, ob die Systemvoraussetzungen für die vorgesehene Software ausreichend dimensioniert sind.

SE-A6 Bereitstellung von Patches, Updates und Änderungen

1) Es MUSS sichergestellt sein, dass sicherheitskritische Patches und Updates für die entwickelte Software zeitnah durch die Entwickler bereitgestellt werden.
2) Werden für verwendete externe Bibliotheken sicherheitskritische Updates bereitgestellt, dann MÜSSEN die Entwickler ihre Software hierauf anpassen und ihrerseits entsprechende Patches und Updates zur Verfügung stellen.

SE-A7 Versionsverwaltung des Quellcodes

1) Der Quellcode des Entwicklungsprojekts MUSS über eine geeignete Versionsverwaltung verwaltet werden.
2) Es MUSS sichergestellt sein, dass durch die Versionsverwaltung alle Änderungen am Quellcode nachvollzogen und rückgängig gemacht werden können.
3) Es MUSS eine Datensicherung der Versionsverwaltung erfolgen.

SE-A8 Überprüfung von externen Komponenten

1) Unbekannte externe Komponenten, deren Sicherheit nicht durch etablierte und anerkannte Peer-Reviews oder vergleichbares sichergestellt werden kann, MÜSSEN auf Schwachstellen überprüft werden.
2) Die Integrität von externen Komponenten MUSS durch Prüfsummen oder kryptographische Zertifikate überprüft werden.

Kapitel 3: Sicherheitsanforderungen an Webanwendungen

WA-A1 Authentisierung bei Webanwendungen

1) Es MÜSSEN die Anforderungen SE-A2 Authentisierung erfüllt werden.

WA-A2 Protokollierung sicherheitsrelevanter Ereignisse von Webanwendungen

1) Es MÜSSEN die Anforderungen SE-A3 Protokollierung sicherheitsrelevanter Ereignisse erfüllt werden.

WA-A3 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

1) Die Webanwendung MUSS ein regelmäßiges Einspielen sicherheitsrelevanter Patches und Updates ermöglichen.

WA-A4 Sichere Konfiguration der Webanwendung

1) Webanwendungen SOLLTEN so konfiguriert sein, dass auf ihre Ressourcen und Funktionen ausschließlich über die vorgesehenen, abgesicherten Kommunikationspfade zugegriffen werden kann. Falls dies nicht möglich ist, MUSS der Zugriff so weit wie möglich eingeschränkt werden.
2) Der Zugriff auf nicht benötigte Ressourcen und Funktionen SOLLTE deaktiviert werden. Falls dies nicht möglich ist, MUSS der Zugriff so weit wie möglich eingeschränkt werden.
3) Folgendes MUSS bei der Konfiguration von Webanwendungen und Webservices umgesetzt werden:
    - Deaktivieren nicht benötigter HTTP-Methoden
    - Konfigurieren der Zeichenkodierung
    - Vermeiden von sicherheitsrelevanten Informationen in Fehlermeldungen und Antworten
    - Speichern von Konfigurationsdateien außerhalb des Web-Root-Verzeichnisses sowie
    - Festlegen von Grenzwerten für Zugriffsversuche

WA-A5 Zugriffskontrolle bei Webanwendungen

1) Es MUSS mittels einer Autorisierungskomponente sichergestellt werden, dass Benutzer nur Aktionen durchführen können, zu denen sie berechtigt sind.
2) Jeder Zugriff auf geschützte Inhalte und Funktionen MUSS durch die Autorisierungskomponente kontrolliert werden, bevor er ausgeführt wird.
3) Es MÜSSEN alle von der Webanwendung verwalteten Ressourcen von der Autorisierungskomponente berücksichtigt werden.
4) Die Benutzer MÜSSEN serverseitig und zentral auf einem vertrauenswürdigen IT-System autorisiert werden.
5) Ist die Zugriffskontrolle fehlerhaft, MÜSSEN Zugriffe abgelehnt werden.
6) Es MUSS eine Zugriffskontrolle bei URL-Aufrufen und Objekt-Referenzen geben.
7) Der Zugriff auf Dateien durch die Benutzer MUSS mit restriktiven Dateisystemberechtigungen beschränkt werden.
8) Es MUSS ein sicherer Umgang mit temporären Dateien vorgesehen werden.

WA-A6 Sicheres Session-Management

1) Session-IDs MÜSSEN zufällig und mit ausreichender Entropie erzeugt werden.

2) Falls das Framework der Webanwendung Session-IDs generieren kann, MUSS diese Funktion des Frameworks verwendet werden. Sicherheitsrelevante Konfigurationsmöglichkeiten des Frameworks MÜSSEN berücksichtigt werden.
3) Die Session-ID MUSS ausreichend geschützt werden, wenn sie übertragen und vom Client gespeichert wird.
4) Eine Webanwendung MUSS den Benutzern die Möglichkeit geben, eine bestehende Sitzung explizit zu beenden.
5) Nachdem sich der Benutzer angemeldet hat, MUSS eine bereits bestehende Session-ID durch eine neue ersetzt werden.
6) Sitzungen MÜSSEN eine maximale Gültigkeitsdauer besitzen (Timeout).
7) Inaktive Sitzungen MÜSSEN automatisch nach einer bestimmten Zeit ungültig werden.
8) Nachdem die Sitzung ungültig ist, MÜSSEN alle Sitzungsdaten sowohl server- als auch clientseitig ungültig und gelöscht sein.

WA-A7 Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen

1) Es MUSS sichergestellt werden, dass eine Webanwendung ausschließlich vorgesehene Daten und Inhalte einbindet und an den Benutzer ausliefert.
2) Falls eine Webanwendung eine Upload-Funktion für Dateien anbietet, MUSS diese Funktion so weit wie möglich eingeschränkt werden (z.B. Beschränkung auf definierte Dateiformate, Beschränkung auf definierte Dateigrößen, Beschränkung auf definierte Anzahl gleichzeitiger Uploads). Zugriffs- und Ausführungsrechte MÜSSEN in diesem Fall restriktiv gesetzt werden. Es MUSS sichergestellt werden, dass ein Benutzer Dateien nur im vorgegebenen Pfad speichern kann.
3) Die Ziele der Weiterleitungsfunktion einer Webanwendung MÜSSEN ausreichend eingeschränkt werden, sodass Benutzer ausschließlich auf vertrauenswürdige Webseiten weitergeleitet werden.
4) Verlässt ein Benutzer die Vertrauensdomäne, MUSS ihn die Webanwendung darüber informieren.

WA-A8 Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen

1) Webanwendungen MÜSSEN vor automatisierten Zugriffen geschützt werden. Dabei MUSS jedoch berücksichtigt werden, wie sich die Schutzmechanismen auf die Nutzungsmöglichkeiten berechtigter Benutzer auswirken.
2) Wenn die Webanwendung RSS-Feeds oder andere Funktionen enthält, die explizit für die automatisierte Nutzung vorgesehen sind, MUSS dies ebenfalls bei der Konfiguration der Schutzmechanismen berücksichtigt werden.

WA-A9 Schutz vor Standardbedrohungen

1) Die folgenden Standardbedrohungen MÜSSEN bei der Entwicklung der Webanwendung beachtet werden:
    - SQL-Injection und andere Command-Injections
    - Cross-Site-Scripting,
    - Cross-Site-Request-Forgery
    - Sitzungsübernahme
    - Rechteausweitung
    - Bad credential Management
    - Manipulierte Cookies und Header
    - Buffer Overflow

2) Werden Daten an ein Datenbank-System weitergeleitet, MÜSSEN Stored Procedures bzw. Prepared SQL Statements eingesetzt werden, wenn dies von der Einsatzumgebung unterstützt wird. Wenn weder Stored Procedures noch Prepared SQL Statements eingesetzt werden können, MÜSSEN die SQL-Queries separat abgesichert werden.

WA-A10 Schutz vertraulicher Daten

1) Durch Direktiven MUSS gewährleistet werden, dass Webanwendung clientseitig keine schützenswerten Daten zwischenspeichern.
2) Es MUSS sichergestellt werden, dass in Formularen keine vertraulichen Formulardaten im Klartext angezeigt werden.
3) Dateien mit Quelltexten der Webanwendung MÜSSEN vor unerlaubten Abrufen geschützt werden.

WA-A11 Umfassende Eingabevalidierung und Ausgabekodierung

1) Alle an eine Webanwendung übergebenen Daten MÜSSEN als potenziell gefährlich behandelt und geeignet gefiltert werden.
2) Alle Eingabedaten sowie Datenströme und Sekundärdaten wie z. B. Session-IDs MÜSSEN validiert werden.
3) Fehleingaben SOLLTEN möglichst nicht automatisch behandelt werden (Sanitizing). Lässt es sich jedoch nicht vermeiden, MUSS Sanitizing sicher umgesetzt werden.
4) Ausgabedaten MÜSSEN so kodiert werden, dass schadhafter Code auf dem Zielsystem nicht interpretiert oder ausgeführt wird.

Kapitel 4: Sicherheitsanforderungen an Webserver

WS-A1 Authentisierung bei Webservern

1) Es MÜSSEN die Anforderungen SE-A2 Authentisierung erfüllt werden.

WS-A2 Protokollierung sicherheitsrelevanter Ereignisse von Webservern

1) Es MÜSSEN die Anforderungen SE-A3 Protokollierung sicherheitsrelevanter Ereignisse erfüllt werden.

WS-A3 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

1) Der Webserver MUSS ein regelmäßiges Einspielen sicherheitsrelevanter Patches und Updates ermöglichen.

WS-A4 Sichere Konfiguration eines Webservers

1) Den Webserver-Prozess MUSS ein Benutzerkonto mit minimalen Rechten zuweisen werden.
2) Der Webserver MUSS in einer gekapselten Umgebung ausgeführt werden, sofern dies vom Betriebssystem unterstützt wird. Ist dies nicht möglich, SOLLTE jeder Webserver auf einem eigenen physischen oder virtuellen Server ausgeführt werden.
3) Dem Webserver-Dienst MÜSSEN alle nicht notwendige Schreibberechtigungen entzogen werden.
4) Nicht benötigte Module und Funktionen des Webservers MÜSSEN deaktiviert werden.

WS-A5 Schutz der Webserver-Dateien

1) Alle Dateien auf dem Webserver, insbesondere Skripte und Konfigurationsdateien, MÜSSEN vor unbefugtem Lesen und Ändern geschützt werden.
2) Es MUSS sichergestellt werden, dass Webanwendungen nur auf einen definierten Verzeichnisbaum zugreifen können (WWW-Wurzelverzeichnis).
3) Der Webserver MUSS so konfiguriert sein, dass er nur Dateien ausliefert, die sich innerhalb des WWW-Wurzelverzeichnisses befinden.
4) Es MÜSSEN alle nicht benötigten Funktionen, die Verzeichnisse auflisten, deaktiviert werden.
5) Es MUSS sichergestellt werden, dass vertrauliche Dateien nicht in öffentlichen Verzeichnissen des Webservers liegen.

WS-A6 Absicherung von Datei-Uploads und -Downloads

1) Alle mithilfe des Webservers veröffentlichten Dateien MÜSSEN vorher auf Schadprogramme geprüft werden.
2) Es MUSS eine Maximalgröße für Datei-Uploads spezifiziert sein.
3) Für Uploads MUSS genügend Speicherplatz reserviert werden.

WS-A7 Verschlüsselung über TLS

1) Der Webserver MUSS für alle Verbindungen durch nicht vertrauenswürdige Netze eine sichere Verschlüsselung über TLS, nach Stand der Technik, anbieten (HTTPS). Falls es aus Kompatibilitätsgründen erforderlich ist, veraltete Verfahren zu verwenden, MÜSSEN diese auf so wenige Fälle wie möglich beschränkt werden.

2) Wenn eine HTTPS-Verbindung genutzt wird, DÜRFEN alle Inhalte NUR über HTTPS verfügbar sein. Sogenannter Mixed Content DARF NICHT verwendet werden
3) Die Empfehlungen der Technischen Richtlinie TR-02102[5] des BSI MÜSSEN beachtet werden.

WS-A8 Schutz vor Denial-of-Service-Angriffen

1) Es MÜSSEN Maßnahmen definiert und umgesetzt werden, die DDoS-Angriffe verhindern oder zumindest abschwächen.

[5] Aktuelle Technische Richtlinie beim BSI: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

Kapitel 5: Sicherheitsanforderung an KI-Entwicklung und KI-Integration

KI-A1 Betriebsdokumentation

1) Es MÜSSEN die zugrunde liegenden Daten und Prozesse der KI-Lösung (z.B. Datengrundlagen der Trainingsdaten; genutzte KI-Modelle, Algorithmen) dokumentiert werden. Dies ist für die Erklärbarkeit der KI zwingend notwendig.

KI-A2 Interventionsmöglichkeit

1) Bei generativer KI: Es MÜSSEN manuelle Kontroll- und Interventionsmöglichkeiten während des Einsatzes der KI-Lösung für Benutzende bestehen (z.B. Verweis auf Quellen).

KI-A3 Sicherung des Versionsverlauf der KI-Lösung

1) Bei hohem Schutzbedarf:
   Vor der Durchführung von Updates der KI-Lösung MUSS die aktuelle Version als Backup an einem sicheren Ort gespeichert werden, auf den nur berechtigte Personen Zugriff haben. Entsprechende Anforderungen können sich aus gesetzlichen Vorgaben ergeben.

KI-A4 Schutz von Test- und Trainingsdaten

1) Die Test- und Trainingsdaten MÜSSEN vor unbefugtem Zugriff und Manipulation nach dem aktuellen Stand der Technik geschützt werden.
2) Es SOLLTEN Versionskontrollen der Daten verwendet werden, um ggf. Manipulationen zu erkennen.

KI-A5 Vorauswahl von Trainingsdaten

1) Zum Training einer KI SOLLTEN keine Echtdaten verwendet werden.
2) Die Verarbeitung personenbezogener Daten SOLLTE zum Trainieren der KI durch Anonymisierung, Pseudonymisierung oder Generalisierung vermieden bzw. begrenzt werden.
3) Echtdaten ab der Informationsklasse "vertraulich" DÜRFEN NICHT in Trainingsdaten verwendet werden.

KI-A6 Trennung von Trainings- / Finetuning- und Nutzungsphase des KI-Modells

1) In der Nutzungsphase MUSS das Training bzw. Fine-Tuning des KI-Modells verhindert werden.

KI-A7 Ausgabeformate definieren und validieren

1) Klare, erwartete Ausgabeformate MÜSSEN für den geplanten Anwendungsfall definiert und beim Testen validiert werden.
2) Es SOLLTE beim Testen deterministischer Code verwendet werden, um die Einhaltung der Ausgabeformate validieren zu können.

KI-A8 Metadatenverarbeitung von Quelldaten

1) Wenn die KI-Lösung Quelldaten verarbeitet, MÜSSEN Anforderungen an die Metadatenverarbeitung definiert und durch die KI-Lösung umgesetzt werden.
   Relevante Metadaten der Quelldaten könnten sein: Informationsklasse, Urheberrechte

Beispiel: KI-Ausgabe enthält Inhalte aus einer Quelldatei mit Informationsklasse "vertraulich" --> generierte KI-Ausgabe erhält den Hinweis, dass vertraulicher Inhalt enthalten ist.

KI-A9 Festlegung von Performanz-Metriken

1) Es MÜSSEN Performanz-Metriken und deren Toleranzgrenze für die Verfügbarkeit der KI-Lösung und die Integrität der Antworten definiert werden.

KI-A10 Monitoring der Performanz-Metriken

1) Es SOLLTE ein Monitoring-System eingerichtet werden, das automatisiert die zuvor definierten Performanz-Metriken überwacht.
2) Falls die KI-Ausgaben nicht dem Maß an erwarteter Leistung entsprechen, MUSS das Monitoring-System eine Warnmeldung aussendet und relevante Beteiligte informieren können.

KI-A11 Einhaltung von Berechtigungen

1) Die KI-Lösung MUSS die Rollen- und Berechtigungsstrukturen der Quelldaten bei der Generierung von KI-Ausgaben zwingend berücksichtigen. Benutzende dürfen nur Zugriff auf für sie zugängliche Daten erhalten.

KI-A12 Rollen- Berechtigungsfunktion bei Grounding

1) Bei der Nutzung von Grounding-Funktionen MUSS eine Rollen- / Berechtigungsfunktion integriert sein, damit die Datenbasis der KI vor Manipulation geschützt wird.

KI-A13 Filterung der Eingabedaten

1) Eingabedaten der Nutzenden (z.B. Prompts) MÜSSEN vor Verarbeitung durch die KI vorgefiltert werden (z.B. Filterung eines Prompts zur Auflistung aller als "vertraulich" gekennzeichneter Daten).

KI-A14 Dokumentation von Datenflüssen und Schnittstellen

1) Alle Datenflüsse und Schnittstellen der KI-Lösung MÜSSEN nachvollziehbar dokumentiert du beschrieben werden.

KI-A15 Absicherung von Schnittstellen

1) Alle Schnittstellen MÜSSEN nach dem aktuellen Stand der Technik abgesichert werden z.B. durch Verschlüsselung und Authentifizierung.

KI-A16 Sperrung von Schnittstellen

1) Bei hohem Schutzbedarf der Vertraulichkeit:
   Die Ausleitung von Eingabedatendaten (z.B. Prompts) an externe Systeme, z.B. Websuch-Dienste zur Anreicherung der Antwort, MUSS zusammen mit dem Auftraggeber (Informationsverantwortlichen bzw. dem verantwortlichen Fachbereich) bewertet und ggf. gesperrt werden.

KI-A17 Kennzeichnung von KI-Ausgaben

1) KI-Ausgaben MÜSSEN durch die KI-Lösung entsprechend den aktuellen gesetzlichen (z.B. KI-Verordnung[6]) bzw. regulatorischen Anforderungen (z.B. KI Guideline) als KI-generierte Inhalte gekennzeichnet werden.

KI-A18 automatisierte Weiternutzung von KI-Ausgaben

1) Eine automatisierte Nutzung und Weiterverarbeitung der KI-Ausgaben MUSS zusammen mit dem Auftraggeber (Informationsverantwortlichen bzw. dem verantwortlichen Fachbereich) bewertet und ggf. gesperrt werden.

KI-A19 Validierung der KI-Ausgabe

1) Die KI-Lösung MUSS die Möglichkeit bieten, dass KI-Ausgaben vor der weiteren Nutzung durch menschliche Kontrolle und Validierung überprüft werden können.

KI-A20 KI spezifische Penetrationstests

1) Bei hohem Schutzbedarf:
   Um Schwachstellen in der KI-Lösung feststellen zu können, MÜSSEN neben den üblichen webbasierten oder infrastrukturellen Penetrationstest auch regelmäßig KI-spezifische Penetrationstests (z.B. Prompt-Injection, Data-Poisoning oder Modelldiebstahl) durchgeführt werden. Je nach Beauftragung MÜSSEN der Auftragnehmer selbst oder der Auftraggeber die Penetrationstests durchführen.

[6] https://eur-lex.europa.eu/legal-content/de/TXT/PDF/?uri=OJ:L_202401689