

Vertragsanlage Informationssicherheit

26-09021

Inhaltsverzeichnis

1 Organisatorische Anforderungen	3
1.1 Anforderungen an die Informationssicherheit	3
1.2 Prüfrechte der TK	3
1.3 Meldung und Aufklärung von Sicherheitsvorfällen	4
1.4 Informationssicherheitsmanagementsystem	4
1.5 Einsatz von Cloud-Computing	4
1.6 Standorte	4
1.7 Datensicherung und Datenexport	4
1.8 Änderung von sicherheitsrelevanten Anforderungen	5
1.9 Pflichten bei Vertragsende	5
2 Technische Anforderungen	6
2.1 Sicherheitsmaßnahmen	6
2.2 Freiheit von Schadsoftware	6
2.3 Endpoint Detection Response (EDR)	6
2.4 Zugriff auf das Active Directory	6
2.5 Benutzerrechtenmanagement	6
2.6 Netzwerksicherheit	7
2.7 Anwendungsschnittstellen	7
2.8 Zugriff auf das Active Directory	7
2.9 Authentifizierung für Mitarbeitende der TK	7
2.10 Andere Anmeldeverfahren des AN	7
2.11 Logging	8
2.12 Patch- und Releasemanagement bei Betrieb durch den AN	8
2.13 Schwachstellenmanagement	9
2.14 Verschlüsselung	9
2.15 Datenlöschung	9

1 Organisatorische Anforderungen

1.1 Anforderungen an die Informationssicherheit

Der AN gewährleistet die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten der TK und verpflichtet sich, angemessene, geeignete technische und organisatorische Maßnahmen zum Schutz der Daten zu ergreifen, die dem aktuellen Stand der Technik entsprechen. Eine regelmäßige Anpassung der IT- Systeme und Prozesse an neue Bedrohungen wird vorausgesetzt.

1.2 Prüfrechte der TK

Die TK ist berechtigt, sich vor Leistungsbeginn und sodann regelmäßig von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Die TK ist berechtigt, regelmäßig (mindestens monatlich, höchstens täglich) oder anlassbezogen (z.B. Bekanntwerden einer über das Netzwerk ausnutzbaren Schwachstelle oder Nachverfolgung von Härtungsmaßnahmen) nichtinvasive Prüfungen wie Portscans und Aufrufe der Webschnittstellen durchzuführen. Darüber hinaus hat die TK das Recht, die Sicherheit der beteiligten Systeme und Prozesse im Rahmen von Assessments zu überprüfen. Insbesondere stimmt der AN zu, dass die TK bzw. ein von Ihr beauftragter Prüfer nach Vorankündigung eigene Penetrationstests durchführen darf.

Auf Anforderung der TK legt der AN Nachweise über die regelmäßige Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen vor.

Darüber hinaus hat die TK das Recht, die Sicherheit der beteiligten Systeme und Prozesse im Rahmen von eigenen Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen selbst zu überprüfen. Die TK ist dazu berechtigt, die Prüfungen durch von Ihr beauftragte Prüfer durchführen zu lassen.

Hierzu hat der AN der TK bzw. einem von der TK beauftragten Prüfer während der normalen Geschäftszeiten Zugang insbesondere zu den für die Verarbeitung der Daten der TK relevanten Verarbeitungssystemen, Einrichtungen sowie zu unterstützenden Unterlagen zu gewähren.

Auf Anforderung der TK unterstützt der AN die TK bei der Durchführung von Audits, Zertifizierungen und Prüfungen, die im Zusammenhang mit den vertragsgegenständlichen Leistungen durchgeführt werden.

Prüfungen können auch durch Aufsichtsbehörden der TK veranlasst werden. Der AN verpflichtet sich, in vollem Umfang mit den für die TK zuständigen Aufsichtsbehörden zu kooperieren. Prüfungen finden mit angemessener Vorankündigung für den AN sowie unter Einhaltung der Geheimhaltung statt. Vor Beginn einer solchen Prüfung teilt die TK den initialen Prüfungsgegenstand und den geplanten Umfang mit, damit der AN entsprechend disponieren kann. Über Ort, Datum und Ansprechpartner stimmen sich die Parteien ab. Ein Abschlussbericht sowie die daraus abgeleiteten Maßnahmen werden dem AN von der TK innerhalb von 90 Tagen bereitgestellt. Jede Partei trägt die ihr entstehenden Kosten für derartige Prüfungen selbst.

1.3 Meldung und Aufklärung von Sicherheitsvorfällen

Der AN hat einen Prozess zur Erkennung, Meldung und Bearbeitung von Sicherheitsvorfällen und Datenschutzverstößen einzurichten und verpflichtet sich, die TK unverzüglich über Vorfälle zu informieren sowie einen detaillierten Bericht über Ursachen, Auswirkungen und Schweregrad des Sicherheitsvorfalls, sowie ergriffene Maßnahmen bereitzustellen. Auch Sicherheitsvorfälle in der vorgelagerten Lieferkette sind der TK zu melden.

Die Meldung muss unverzüglich an den jeweils verantwortlichen Ansprechpartner sowie an die Mailadresse v-Geschaeftpartner-Vorfall@tk.de erfolgen.

Im Falle eines Sicherheitsvorfalls, bei dem es zu einem potenziellen Datenabfluss oder einer potenziellen Kompromittierung von Daten gekommen sein könnte, verpflichtet sich der AN auf eigene Kosten zu einer qualifizierten forensischen Aufarbeitung des Vorfalls durch einen externen Dienstleister. Der AN hat die Ergebnisse dieser Aufarbeitung der TK schnellstmöglich zur Verfügung zu stellen, insbesondere in welchem Umfang Daten von TK-Versicherten betroffen sind.

Der AN stellt der TK auf Anforderung alle erforderlichen Informationen bereit, welche die TK zur Erfüllung ihrer Meldepflichten gegenüber Behörden sowie zur Befolgung etwaiger Herausgabepflichten benötigt.

1.4 Informationssicherheitsmanagementsystem

Der AN verpflichtet sich, ein Informationssicherheitsmanagementsystem (ISMS) gemäß anerkannten Standards wie der ISO/IEC 27001 oder vergleichbaren Standards/Normen (z.B. BSI IT-Grundschutz) zu implementieren, aufrechtzuerhalten und regelmäßig in angemessener Form zu überprüfen.

1.5 Einsatz von Cloud-Computing

Sofern der AN im Rahmen der Leistungserbringung Cloud-Computing Dienste nutzt, erbringt er die Leistungen unter Beachtung der bei Vertragsschluss jeweils aktuellen Anforderungskatalogs C5 (Basiskriterien). Ein Nachweis der Einhaltung aller Anforderungen gegenüber der TK durch ein C5-Testat ist nicht erforderlich.

1.6 Standorte

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung der TK und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

1.7 Datensicherung und Datenexport

Der Auftragnehmer ist verpflichtet, in regelmäßigen Abständen Datensicherungen vorzunehmen. Zudem muss der AN in angemessener Frist eine Wiederherstellung von Daten aus einem Backup auf den von der TK gewünschten vorhandenen Stand vorzunehmen.

Der AN muss über praxiserprobte Backup- und Restore-Konzepte verfügen und diese TK auf Anforderung nachweisen.

Die Leistung ist so auszugestalten, dass die TK jederzeit selbstständig oder, soweit dies aus technischen Gründen nicht möglich ist, mit Unterstützung durch den AN ihre Daten in einem marktüblichen Austauschformat exportieren kann. Damit muss auch der Export von bestimmten Teilen der Daten der TK möglich sein. Soweit die Daten verschlüsselt sind, ist diese Pflicht nur dann erfüllt, wenn die TK auch über den Schlüssel verfügt. Für den Export der Daten und deren Sicherung nach dem Export ist die TK verantwortlich.

1.8 Änderung von sicherheitsrelevanten Anforderungen

Sofern sich sicherheitsrelevante Anforderungen, auf die im Rahmen dieses Vertrages verwiesen wird, während der Vertragslaufzeit ändern, wird der AN auch die neuen bzw. geänderten Anforderungen unaufgefordert innerhalb angemessener Frist, spätestens ab Inkrafttreten oder gegebenenfalls innerhalb der Übergangsfristen, erfüllen.

Sofern dem AN eine Erfüllung der neuen Anforderungen nicht möglich ist, teilt er dies der TK unverzüglich, in jedem Fall innerhalb der vom Gesetzgeber vorgesehenen Umsetzungsfrist, ab Veröffentlichung der neuen Anforderung mit.

1.9 Pflichten bei Vertragsende

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch die TK – spätestens mit Beendigung des Vertrages – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Daten, erstellte Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, der TK auszuhändigen oder nach vorheriger Zustimmung entsprechend der Anforderungen zur Datenlöschung zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

2 Technische Anforderungen

2.1 Sicherheitsmaßnahmen

Der AN muss alle zumutbaren und geeigneten technischen und organisatorischen Maßnahmen ergreifen, die einen unbefugten und missbräuchlichen Zugriff auf die eingesetzten IT-Systeme, Anwendungen, zugehörige Komponenten sowie zugehörige Daten unterbinden. Die getroffenen Maßnahmen müssen dabei dem aktuellen Stand der Technik entsprechen.

Der Einsatz von kritischen Komponenten deren Einsatz gemäß BSIG §41 vom BMI untersagt wurde, ist nicht erlaubt. Zur Vertragslaufzeit betroffene Komponenten müssen unverzüglich durch den AN ausgetauscht werden.

Sollten sich aufgrund neuer Erkenntnisse oder Bedrohungen Sicherheitslücken ergeben, so muss der AN diese unverzüglich der TK anzeigen und sie durch geeignete Maßnahmen beseitigen. Sofern die Maßnahmen die Verfügbarkeit, der für die TK zur Verfügung gestellten Dienste beeinflussen, muss der AN diese mit der TK abstimmen.

2.2 Freiheit von Schadsoftware

Alle Bestandteile der erbrachten Leistung müssen frei von Schadsoftware sein. Der AN muss dies durch geeignete Maßnahmen sicherstellen. Der AN muss insbesondere beteiligte IT-Systeme und Software mittels eines marktgängigen und aktuellen Scanners oder mindestens gleichwertiger Technologie prüfen.

2.3 Endpoint Detection Response (EDR)

Die bereitgestellte IT-Komponente des AN muss in die zentrale EDR-Sicherheitslösung der TK integriert werden können. Die dafür benötigten Lizenzen werden nach Abstimmung von der TK bereitgestellt.

Falls dies nicht möglich ist, muss die IT-Komponente eine eigene EDR-Sicherheitslösung mitbringen, deren Logs an das SIEM der TK gesendet werden können.

2.4 Zugriff auf das Active Directory

Zugriffe auf das Active Directory per LDAP erfolgen weder anonym noch mit Gast-Identität und müssen dafür TLS-Verschlüsselung (also LDAPS) verwenden

2.5 Benutzerrechtenmanagement

Der AN hat sicherzustellen, dass der Zugriff auf Systeme, Anwendungen und Daten/Informationen ausschließlich autorisierten Personen nach dem Prinzip der minimalen Rechtevergabe gewährt wird und geeignete technische Maßnahmen wie Zwei-Faktor- bzw. Multi-Faktor-Authentifizierung implementiert sind. Der AN muss für sicherheitsrelevante Prozesse das Vier-Augen-Prinzip umsetzen. Die vorhandenen Rollen und Rechte sind in einem Berechtigungskonzept zu beschreiben und auf Wunsch der TK vorzulegen.

2.6 Netzwerksicherheit

Der AN stellt sicher, dass er seine angebotenen Dienste netzwerkseitig angemessen schützt. Dazu gehört eine Segmentierung der Netzwerke entsprechend der fachlichen Notwendigkeit und die Etablierung eines feingranularen Regelwerks zur Beschränkung des Netzwerkverkehrs auf die zur Leistungserbringung notwendigen Dienste.

2.7 Anwendungsschnittstellen

Der AN stellt sicher, dass externe Schnittstellen (APIs) der bereitgestellten Anwendungen angemessen gegen unbefugte Nutzung geschützt sind.

2.8 Zugriff auf das Active Directory

Zugriffe auf das Active Directory per LDAP erfolgen weder anonym noch mit Gast-Identität und müssen dafür TLS-Verschlüsselung (also LDAPS) verwenden.

2.9 Authentifizierung für Mitarbeitende der TK

Die Anwendung ist in ein Single Sign On bei der TK integrierbar. Es wird das Microsoft Active Directory oder Entra ID bei der Anmeldung unterstützt.

Zur Authentifizierung wird mindestens eines der folgenden Protokolle unterstützt:

- OpenID/OAuth2 über Microsoft Entra ID Enterprise Application (siehe <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-application-management>)
- SAML über Microsoft Entra ID Enterprise Application (siehe <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-application-management>)
- Kerberos über Microsoft Active Directory. Dies ist jedoch NICHT zulässig für Anwendungen, die über eine HTTP-Schnittstelle angesprochen werden. In diesem Fall unterstützt die Anwendung mindestens eines der beiden anderen genannten Protokolle.

Die Anwendung verfügt über ein für den Anwendungszweck geeignetes Rollen- und Rechte-Management. Dieses stellt insbesondere sicher, dass:

- Die Rechte für administrative Tätigkeiten von den Rechten zur regulären Nutzung getrennt sind.
- Auf von der Anwendung verarbeitete Daten nur von denjenigen Mitarbeitern zugegriffen werden kann, die den Zugriff für die Erfüllung ihrer Aufgaben benötigen.

2.10 Andere Anmeldeverfahren des AN

Sofern die Anwendung eine eigene Authentifizierung implementiert, welche nicht an einen Authentifizierungsdienst angebinden ist und bei der Authentifizierung geheimes Wissen (Kennwörter, Passwörter, PINs, etc.) verwendet, gelten nachfolgende Anforderungen:

- Die Authentifizierung muss die Anzahl von Fehlversuchen wirksam begrenzen.
- Die Authentifizierung muss die Auswahl von trivialen Geheimnissen durch Anwendende verhindern.

Anforderungen an Geheimnisse:

- Falls das Geheimnis systemseitig generiert wird, soll es durch einen technischen Prozess mindestens annähernd zufällig erzeugt werden.
- Sofern die Authentifizierung nicht für Offline-Angriffe anfällig ist, muss es mindestens 8-stellig sein.
- Sofern die Authentifizierung anfällig für Offline-Angriffe ist, muss das Geheimnis mindestens 12-stellig sein.
- Sofern es eine Maximallänge für Geheimnisse gibt, so muss diese mindestens 64 Stellen sein.
- Führende und abschließende Leerzeichen sollen verhindert werden, aber Leerzeichen innerhalb des Geheimnisses sollen erlaubt sein.
- Alle Zeichen der Klassen Großbuchstabe, Kleinbuchstabe, Ziffer und druckbare Sonderzeichen sollen verwendbar sein.
- Mindestens drei der vier Zeichenklassen müssen für Geheimnisse verwendet werden.
- Falls technisch bedingt nur ein geringerer Zeichensatz möglich ist, muss die Mindestlänge des Geheimnisses entsprechend erhöht werden.
- Bei einem Geheimniswechsel muss das aktuelle Geheimnis abgefragt werden. Es darf nicht als neues Geheimnis auswählbar sein.

Die Geheimnisse dürfen niemals im Klartext gespeichert werden. Gespeicherte Geheimnisse sind mittels Passworthashingalgorithmen wie PBKDF2 oder Argon2 oder vergleichbar sicheren Verfahren zu schützen.

2.11 Logging

Zugriffe auf sensible oder sozialversicherungsrechtliche Daten sowie administrative Zugriffe und das Starten von Batch-Prozessen müssen mittels Logging protokolliert werden.

Das Logging soll mittels der Logging Facility der jeweiligen Plattform (bspw. Windows- Eventlog, Syslog) erfolgen. Sofern die Logging Facility der jeweiligen Plattform nicht verwendet wird, müssen Logeinträge in Dateien oder Datenbanken gespeichert werden.

Logeinträge müssen maschinell auswertbar sein. Über das Format der Logeinträge muss ab Leistungsbeginn eine vollständige und verständliche Dokumentation geliefert werden.

Sämtliche Logeinträge müssen einen Zeitstempel enthalten. Der Zeitstempel muss auf der Betriebssystemzeit beruhen oder es muss anderweitig sichergestellt werden, dass die Abweichung zu einer offiziellen Zeitquelle (z. B. einem NTP-Server) weniger als 3 Sekunden beträgt.

Sofern die Logeinträge nicht in von Menschen lesbarer und verständlicher Form für Revisionszwecke vorliegen, müssen entsprechende Aufbereitungsprogramme zur Verfügung gestellt werden.

Logdaten müssen vor unberechtigten Zugriffen geschützt sein.

2.12 Patch- und Releasemanagement bei Betrieb durch den AN

Bei einem Betrieb von IT-Komponenten durch den AN muss dieser über einen Patch-Management-Prozess verfügen, dass alle von ihm eingesetzten Systeme, Systemkomponenten und Entwicklungswerkzeuge jeweils auf einem aktuellen Versionsstand und insbesondere frei von Schwachstellen sind. Der AN muss sicherstellen, dass je nach Risiko für die Anwendung (bewertet durch den AN) Sicherheitspatches - innerhalb von 1-5 Arbeitstagen nach Veröffentlichung des Patches eingespielt werden.

2.13 Schwachstellenmanagement

Der AN betreibt ein aktives Schwachstellenmanagement. Es werden regelmäßig geplant Schwachstellenscans auf den eingesetzten IT-Systemen durchgeführt und die Ergebnisse in einem risikobasierten Ansatz zur Verbesserung der Sicherheitsmaßnahmen verwendet.

Wenn der AN Leistungen im Rahmen des öffentlichen Internetauftritts der TK erbringt (Nutzung Public IPs, (Sub-)Domänen) ist die Leistung an das Schwachstellenmanagement der TK anzubinden.

2.14 Verschlüsselung

Alle Daten der TK müssen sowohl bei der Speicherung als auch beim Transport verschlüsselt werden.

Sofern in der Software Verschlüsselungsalgorithmen eingesetzt werden, sind diese zur aktuellen Fassung der *BSI TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“* konform. Sofern Verschlüsselungsalgorithmen im direkten Umfeld von qualifizierten elektronischen Signaturen nach dem bundesdeutschen Signaturgesetz eingesetzt werden, richten sie sich nach den Veröffentlichungen der Bundesnetzagentur im Bundesanzeiger. Verschlüsselungsverfahren werden vor Ablauf des laut der o.a. genannten Vorschriften zulässigen Verwendungsdatums durch aktuelle Verfahren ersetzt werden.

Sofern TLS zur Transportverschlüsselung eingesetzt wird, hält sich der AN bei der Wahl von TLS-Version(en) und der einzusetzenden Cipher-Suites an die Empfehlungen der jeweils aktuellen Fassung der Technischen Richtlinie *BSI TR-02102-2 “Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)”* des BSI. Der AN stellt sicher, dass alle Kommunikationsteilnehmer mindestens eine der zulässigen Cipher-Suites unterstützen. Der AN gleicht die von ihm gewählte Konfiguration mindestens jährlich gegen die Vorgaben des BSI ab. Bei Bedarf passt der AN die Konfiguration an, um Konformität mit der o.a. Technischen Richtlinie herzustellen.

Sollen sicherheitsrelevante Zufallswerte (z.B. Session-IDs, kryptographisches Material, Initial-PINs) in einer Anwendung verwendet werden, so müssen diese hinreichend zufällig sein. Die dafür verwendeten Zufallsgeneratoren müssen den Vorgaben aus Kapitel "Zufallszahlengeneratoren" der aktuellen Technischen Richtlinie *BSI TR-02102-1* des BSI entsprechen.

2.15 Datenlöschung

Bei der Verwendung von SaaS werden Storage-Komponenten (die zur persistenten Speicherung von Daten verwendet werden) bei Außerbetriebnahme einer Appliance, des Services und bei der Beendigung des Vertrages gelöscht. Die Löschung einer Speicherkomponente entspricht einer physischen Vernichtung. Die Löschung aller virtuellen Ressourcen muss in einem Protokoll dokumentiert werden. Dieses Protokoll muss der TK zur Verfügung gestellt werden. Gelöschte Speicherressourcen dürfen nicht wiederherstellbar sein.

Bei der Außerbetriebnahme einer Appliance, bei Austausch von Hardware-Komponenten sowie bei der Beendigung eines Vertrages und vor der Wiederverwendung von Speichermedien durch andere Kunden des AN, müssen alle permanent speichernden Datenträger sicher vernichtet oder sicher gelöscht werden. Eine Weitergabe oder Rückgabe an Dritte, ausgenommen zur professionellen Löschung bzw. Vernichtung, darf nicht stattfinden. Der AN muss über

die erfolgte Vernichtung/Löschung ein Protokoll anfertigen, aus dem hervorgeht, wann und mittels welchen Verfahrens die Datenträger vernichtet/gelöscht wurden. Der AN muss der TK das Protokoll auf Anforderung zur Verfügung stellen.

Für Datenträger mit folgenden Kriterien muss eine Vernichtung erfolgen. Löschen ist unzulässig bei defekten Datenträgern und Wechselmedien (USB-Sticks, Speicherkarten, etc.).

Eine Vernichtung muss gemäß folgender Vorgaben oder gleich-/höherwertiger Verfahren erfolgen:

- Festplatten (HDD): DIN 66399-2, mindestens Stufe H-4
- Solid State Disks (SSD), Hybridfestplatten (SSHD), Wechselmedien: DIN 66399-2, mindestens Stufe E-4

Bei allen funktionsfähigen, verschlüsselten magnetischen Datenträgern kann eine elektronische sichere Löschung durchgeführt werden. Dabei muss die Löschung auf dem gesamten Datenträger nach dem nachfolgenden Löschverfahren erfolgen:

1. Löschfunktion des Laufwerks (ATA "Secure Erase")
2. DoD 5220.22-M (ECE) bzw. gleich-/höherwertig
3. Löschfunktion des Laufwerks (ATA "Secure Erase")

Bei allen funktionsfähigen, verschlüsselten halbleiterbasierten Datenträgern kann eine elektronische sichere Löschung durchgeführt werden. Dabei muss die Löschung auf dem gesamten Datenträger nach einem der nachfolgenden Löschverfahren erfolgen:

- Verfahren 1:
 1. Löschfunktion des Mediums (ATA-"Secure-Erase")
 2. Überschreiben des gesamten Speichers
 3. Löschfunktion des Mediums (ATA-"Secure-Erase")
- oder Verfahren 2:
 1. Löschen des Schlüssels für die Festplattenverschlüsselung im TPM-Chip
 2. Überschreiben des gesamten Speichers
 3. Löschen des Schlüssels für die Festplattenverschlüsselung im TPM-Chip