Vertragsanlage V3

Informationssicherheit

25-08897 Sektoraler Identity Provider (IDP)

Version:	1.0 (Final und freigegeben)
Datum:	13.03.2026
Eigentümer:in:	TK
Klassifizierung der Vertraulichkeit:	C1 - Intern
Dokumentenreferenzname:	TK_Vertragsanlage_Informationssicherheit

Inhaltsverzeichnis

1 Organisatorische Anforderungen 3

1.1 Vorrang von Anforderungen 3
1.2 Grundlegende Anforderungen an die Informationssicherheit 3
1.3 Prüfrechte 3
1.4 Prüfung durch Aufsichten 3
1.5 Meldung und Aufklärung von Sicherheitsvorfällen 4
1.6 Änderung von sicherheitsrelevanten Anforderungen 4
1.7 Pflichten bei Vertragsende 4
1.8 Informationssicherheitsmanagementsystem 4
1.9 Business Continuity Management- / Notfallmanagement 5
1.10 Einsatz von Cloud-Computing 5
1.11 Standorte 5
1.12 Schulung und Sensibilisierung 5

2 Technische Anforderungen 6

2.1 Sicherheitsmaßnahmen 6
2.2 Freiheit von Schadsoftware 6
2.3 Systeme zur Angriffserkennung 6
2.4 Authentifizierung für Mitarbeitende der TK 6
2.5 Benutzerrechtemanagement 6
2.6 Netzwerksicherheit 7
2.7 Anwendungsschnittstellen 7
2.8 Anforderungen an Softwareentwicklung & -bereitstellung 7
2.9 Bereitstellung von Apps 7
2.10 Bestandteile der Software (SBOM) 8
2.11 Logging / Protokollierung 8
2.12 Patch- und Release-Management 8
2.13 Schwachstellenmanagement 9
2.14 Verschlüsselung 9
2.15 Datenlöschung 9

1 Organisatorische Anforderungen

1.1 Vorrang von Anforderungen

Zu dem Leistungsgegenstand dieses Vertrages gibt es eine Vielzahl von Anforderungen der Gematik, des BSI und von individuellen Vorgaben der TK in der Leistungsbeschreibung. Falls eine allgemeine organisatorische oder technische Anforderung aus diesem Dokument in einem direkten Widerspruch zu den o.g. Vorgaben stehen sollte, haben die o.g. Anforderungen Vorrang.

1.2 Grundlegende 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 dynamische Bedrohungsumfelder wird vorausgesetzt.

1.3 Prüfrechte

Die TK ist berechtigt, sich vor Leistungsbeginn und sodann regelmäßig, aber höchsten einmal jährlich, von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

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.

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.

1.4 Prüfung durch Aufsichten

Der AN verpflichtet sich, in vollem Umfang mit den für die TK zuständigen Aufsichts- und Abwicklungsbehörden zu kooperieren. Dies umfasst die Bereitstellung von Dokumentationen, Berichtserstattungen und die Teilnahme an Besprechungen, die von den Behörden initiiert oder angeordnet werden. Der AN wird die TK unverzüglich über alle Anfragen, Prüfungen oder Ermittlungen von Seiten der Behörden informieren, die sich auf die erbrachten IT-Dienstleistungen oder die verarbeiteten Daten beziehen. Alle Antworten und erforderlichen

Dokumente sind im Vorfeld mit der TK abzustimmen, um sicherzustellen, dass die Interessen der TK gewahrt bleiben.

1.5 Meldung und Aufklärung von Sicherheitsvorfällen

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

Die Meldung muss unverzüglich an den verantwortlichen Ansprechpartner seitens der TK sowie an die Mailadresse v-Geschaeftspartner-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 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.

1.6 Änderung von sicherheitsrelevanten Anforderungen

Sofern sich sicherheitsrelevante Anforderungen, auf die im Rahmen dieser Vertragsvereinbarung verwiesen wird, während der Laufzeit ändern, wird der AN auch die neuen bzw. geänderten Anforderungen unaufgefordert innerhalb angemessener Frist erfüllen.

Sollte der AN innerhalb von zwölf Monaten (vorbehaltlich einer anderen vom Gesetzgeber vorgegebenen Umsetzungsfrist, die in jedem Fall einzuhalten ist) ab der Veröffentlichung der neuen Anforderungen erklären, dass er die neuen Anforderungen nicht erfüllt, hat die TK ein Sonderkündigungsrecht.

1.7 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 (Abs. 1.6) zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung der TK vorzulegen.

1.8 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.

Ein entsprechendes, aktuell gültiges, Zertifikat ist mindestens jährlich gegenüber der TK nachzuweisen. Bei unterjährigen - für die TK relevanten - Änderungen des Zertifikats ist die TK unverzüglich zu informieren.

1.9 Business Continuity Management- / Notfallmanagement

Der AN ist verpflichtet, ein Business Continuity Management (BCM) gemäß anerkannten Standards wie der ISO/IEC 22301 oder vergleichbaren Standards/Normen (z.B. BSI IT-Grundschutz 200-4) zu etablieren, regelmäßig zu testen und sicherzustellen, dass im Falle von Betriebsstörungen eine ausreichend schnelle Wiederherstellung gemäß des vereinbarten SLA für die erbrachten Leistungen gewährleistet ist.

Bezüglich der erbrachten Leistung müssen durch den AN Notfallpläne erstellt und mit der TK abgestimmt werden.

1.10 Einsatz von Cloud-Computing

Sofern der AN Cloud-Computing zur Leistungserbringung einsetzt, müssen die Leistungen unter Einhaltung der Anforderungen des § 393 SGB V und der zugehörigen C5-Gleichwertigkeitsverordnung erbracht werden.

Ein aktuell gültiges C5-Testat ist mindestens jährlich gegenüber der TK nachzuweisen. Bei unterjährigen - für die TK relevanten - Änderungen des Testats ist die TK unverzüglich zu informieren.

1.11 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.

1.12 Schulung und Sensibilisierung

Der AN ist verpflichtet, Mitarbeitende regelmäßig über Informationssicherheitsanforderungen zu schulen und sicherzustellen, dass die für die Leistungserbringung eingesetzten Mitarbeitenden die notwendigen Kenntnisse zur Einhaltung der vertraglich vereinbarten Sicherheitsstandards besitzen.

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 Systeme zur Angriffserkennung

Der Einsatz von Systemen zur Angriffserkennung entsprechend des Mindeststandards des BSI für Systeme zur Angriffserkennung in der jeweils aktuell gültigen Version ist seitens des AN verpflichtend.

2.4 Authentifizierung für Mitarbeitende der TK

Es muss das Microsoft Active Directory oder EntraID bei der Anmeldung unterstützt werden. Die Anwendung muss in ein Single Sign On bei der TK integriert werden können.

Zur Authentifizierung soll mindestens eines der folgenden Protokolle unterstützt werden:

- Kerberos
- SAML über Entra ID Enterprise Application
- OAuth2 über Entra ID Enterprise Application

Die Anwendung muss über ein für den Anwendungszweck geeignetes Rollen- und Rechte-Management verfügen, welches sicherstellt, dass auf personenbezogene Daten nur von denjenigen Mitarbeitern zugegriffen werden kann, die den Zugriff für die Erfüllung ihrer Aufgaben benötigen. Die Rollen des Berechtigungssystems sollen sich aus Mitgliedschaften in AD- bzw. Azure-AD Gruppen ableiten lassen.

2.5 Benutzerrechtemanagement

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.

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 Dienste/Anwendungen angemessen geschützt sind gegen unberechtigte Nutzung.

2.8 Anforderungen an Softwareentwicklung & -bereitstellung

Der AN ist verpflichtet im Rahmen der für die TK erbrachten Software-Entwicklungsleistung folgende Aspekte zu beachten:

- Grundsätzlich ist der Prüfkatalog im Bereich der App-Entwicklungen der deutschen Datenschutzaufsichtsbehörden und die BSI TR-03161 zu berücksichtigen.
- Die Entwicklung der beauftragten Software der TK von den Entwicklungsprojekten anderer Kunden des AN getrennt sein.
- Im Rahmen der Softwareentwicklung sind die Prämissen Least Functionality, Security by Design und Privacy by Design zu berücksichtigen.
- Es muss eine Dokumentation für die Anwendung bereitgestellt werden.
- Es müssen standardmäßig und strukturiert im Rahmen des Entwicklungsprozesses Modul-, Integrations-, Sicherheits- und Abnahmetests durchgeführt und protokolliert werden.
- Tests inkl. Dokumentation der Testfälle und -ergebnisse
- Statische und dynamische Verfahren zum Aufspüren von Schwachstellen in eigenentwickeltem Code
- Verfahren zur Erkennung von Schwachstellen in verwendeten Drittanbieterkomponenten
- Überprüfen von Code-Qualitätsstandards in eigenentwickeltem Code
- Change-Management inkl. Freigabeverfahren
- Problem-Management inkl. Lösungen und Maßnahmen zur künftigen Prävention
- Vor einer Produktivsetzung der entwickelten Software muss ein Penetrationstest durchgeführt werden. Eventuelle Befunde müssen behoben werden und die Ergebnisse sind der TK mitzuteilen.

2.9 Bereitstellung von Apps

Die App muss die Fähigkeit haben, Updates zu erzwingen, damit der Nutzer die jeweils neueste Version der App verwendet. Nutzer einer veralteten App-Version müssen beim Start der App aktiv aufgefordert werden, die App zu aktualisieren. Eine Nutzung der App in der veralteten Version darf nicht möglich sein.

2.10 Bestandteile der Software (SBOM)

Der AN ist zur Lieferung einer SBOM (Software Bill of Materials) für die eingesetzte Software verpflichtet. SBOM ist eine formale, strukturierte Aufzeichnung, die die Artefakte einer Software identifiziert und ihre Beziehungen untereinander und zu anderer Software/anderen Artefakten beschreibt. Diese muss für jede Standardsoftware und jeden Bestandteil gemäß BSI TR-03183-2 bereitgestellt werden.

2.11 Logging / Protokollierung

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 Release-Management

Jegliche eingesetzte oder selbst entwickelte Software muss gepflegt werden. Dazu gehört eine regelmäßige Anpassung an die aktuelle Bedrohungslage durch Schwachstellen und neue Anforderungen.

Der AN informiert die TK selbstständig und ohne Aufforderung schriftlich über neue Versionen und Patches.

Sicherheitsrelevante Patches auf Plattform- und Datenbankebene müssen spätestens 2 Wochen nach deren genereller Verfügbarkeit unterstützt werden. Service Packs und neue Maintenance Level auf Plattform- und Datenbankebene müssen spätestens 3 Monate nach der generellen Verfügbarkeit unterstützt werden. Neue Releases auf Plattform- und Datenbankebene müssen spätestens 12 Monate nach deren genereller Verfügbarkeit unterstützt werden.

Sofern Anwendungskomponenten auf Windows-Clientsystemen vorgesehen sind, müssen diese neue Windows-Funktionsupdates innerhalb von 6 Monaten nach genereller Verfügbarkeit unterstützen.

Bei einem Betrieb von IT-Komponenten durch den AN muss dieser über einen Patch-Management-Prozess gewährleisten, 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 1-18 Arbeitstagen nach Veröffentlichung des Patches eingespielt sind.

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.

2.14 Verschlüsselung

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

Sofern TLS zur Transportverschlüsselung eingesetzt wird, muss der AN sich bei der Wahl von TLS-Version(en) und der einzusetzenden Cipher-Suites an die Empfehlungen der jeweils aktuellen Fassung der BSI TR-02102-2 halten. Der AN muss die von ihm gewählte Konfiguration mindestens jährlich gegen die Vorgaben des BSI abgleichen und bei Bedarf anpassen.

Sofern in der Anwendung Verschlüsselung eingesetzt werden, müssen die verwendeten Verschlüsselungsalgorithmen zur aktuellen Fassung der BSI TR-02102-1 konform sein. Sofern Verschlüsselungsalgorithmen im direkten Umfeld von qualifizierten elektronischen Signaturen nach dem bundesdeutschen Signaturgesetz eingesetzt werden, müssen sie sich nach den Veröffentlichungen der Bundesnetzagentur im Bundesanzeiger richten. Verschlüsselungsverfahren müssen vor Ablauf des genehmigten Verwendungsdatums durch aktuelle Verfahren ersetzt werden.

Sollen Zufallszahlen in der Anwendung verwendet werden, so müssen diese – dem Anwendungszweck entsprechend – hinreichend zufällig sein. Als Informationsquelle für zulässige Zufallszahlengeneratoren kann ebenfalls die aktuelle Technischen Richtlinie TR-02102-1 des BSI dienen.

2.15 Datenlöschung

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