

Vertragsanlage V3 Informationssicherheit,
26-09090 Medienbeobachtung und -analyse
Organisatorische Anforderungen

Vertragsanlage Informationssicherheit

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 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.

1.3 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.

1.4 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.

Vertragsanlage V3 Informationssicherheit,
26-09090 Medienbeobachtung und -analyse

Organisatorische Anforderungen

Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

2 Technische Anforderungen

2.1 Authentifizierung für Mitarbeitende der TK

Anwendungen des AN sollen in ein Single Sign On bei der TK integrierbar sein. 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.

2.2 Andere Anmeldeverfahren des AN

Sofern die Anwendung eine eigene Authentifizierung implementiert, welche nicht an einen Authentifizierungsdienst angebunden 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.

Technische Anforderungen

- 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.