# Überblick

*Geben Sie einen kurzen Überblick über die geplante Verarbeitung, ihre Art, ihren Umfang, ihren Kontext, ihre Zwecke und ihre Beteiligten. Identifizieren Sie den Verantwortlichen und alle Auftragsverarbeiter. Listen Sie die für die Verarbeitung geltenden Standards und Normen auf, die erforderlich sind oder eingehaltenwerden müssen, nicht zuletzt die genehmigten Verhaltensregeln (*[vgl. Art. 40 der [DS-GVO]](http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE)*) und Zertifizierungen zum Datenschutz (*[vgl. Art. 42 [DS-GVO]](http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE)*).*

## Welche Verarbeitung ist geplant?

Zuständige Stelle

## Welche Zuständigkeiten bestehen für die Verarbeitung?

Für das technische Verfahren ThAVEL liegt eine gemeinsame Verantwortlichkeit vor. Diese umfasst das Thüringer Finanzministerium, als das für E-Government und IT zuständige Ministerium, und die ThAVEL nutzenden zuständigen Stellen (Ministerien, Landes- und Kommunalbehörden).

Als Auftragsverarbeiter wird zum einem die FJD AG und zum anderen IT.Niedersachsen tätig (Stand: 12/2020). Aufgabe der FJD ist die Bereitstellung von Updates und Patches, sowie die Weiterentwicklung von ThAVEL. IT.Niedersachsen stellt den technischen Betrieb der zugrunde liegenden Infrastruktur sicher.

## Gibt es Normen oder Standards für die Verarbeitung?

Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt, ThürEGovG, ThürDSG, BDSG, DS-GVO, SGB.

Zuständige Stelle

## Welche Daten werden verarbeitet?

Zuständige Stelle

## Wie verläuft der Lebenszyklus von Daten und Prozessen?

Zuständige Stelle

## Mit Hilfe welcher Betriebsmittel erfolgt die Datenverarbeitung?

ThAVEL wird auf Basis der GovOS Plattform der Firma FJD AG betrieben. Diese wird in einem Tomcat-Application-Server auf einem virtuellen Linux-Server in einem Serververbund mit drei Stages betrieben. Zusätzlich wird Java und als Datenbanksystem MySQL eingesetzt.
Die Verbindung ins Internet erfolgt über ein Application Security Gateway.

# Grundlegende Prinzipien

## Sind die Verarbeitungszwecke eindeutig definiert und rechtmäßig?

Zuständige Stelle

## Aufgrund welcher Rechtsgrundlage erfolgt die Verarbeitung?

Der überwiegende Teil der Verarbeitungstätigkeiten erfolgt auf Grundlage des Art. 6 (1) Bst. e) DS-GVO, § 16 (1) ThürDSG. In Einzelfällen ist auch eine Verarbeitung nach Art. 6 (1) Bst. a) DS-GVO denkbar.

Zuständige Stelle

## Sind die erhobenen Daten erforderlich, relevant und auf das für die Datenverarbeitung Notwendige beschränkt?

Zuständige Stelle

## Sind die Daten korrekt und auf dem neuesten Stand?

Zuständige Stelle

## Welche Speicherdauer haben die Daten?

Auf den ThAVEL-Servern werden die Antragsdaten 388 Tage gespeichert. Nach 360 Tagen wird automatisch eine Löschungsankündigung an den Nutzer versandt, welche nach weiteren 28 Tagen vollzogen wird.

Zuständige Stelle

## Wie werden die betroffenen Personen über die Verarbeitung informiert?

Bei ThAVEL handelt es sich um ein Antragsdaten verarbeitendes System, welches durch den Bürger oder dessen gesetzlichen Vertreter genutzt wird. Eine separate Information des Betroffenen erübrigt sich aufgrund dessen.

## Wenn anwendbar, wie wird die Einwilligung der betroffenen Personen eingeholt?

Bei Datenerhebungen welche auf Grundlage des Art. 6 (1) Bst. a) DS-GVO durchgeführt werden, wird systemseitig die Einwilligung durch den ThAVEL-Nutzer abgefragt, welche vor Antragsstellung proaktiv bestätigt werden muss.

## Wie können Betroffene ihre Rechte auf Auskunft und Datenübertragbarkeit ausüben?

Da es sich bei dem überwiegenden Teil der über ThAVEL erhobenen personenbezogenen Daten um hoheitliche Aufgaben handelt, welche durch die Kommunen in gemeinsamer Verantwortlichkeit (Art. 26 DS-GVO) durchgeführt wird, besteht nach Art. 20 (3) DS-GVO das Recht auf Datenübertragbarkeit nicht.

Bei einer Datenverarbeitung auf Grundlage des Art. 6 (1) Bst. a) DS-GVO wird der betroffenen Person das Recht auf Datenübertragbarkeit auf Antrag, durch die zuständige Stelle, gewehrt.

## Wie können betroffene Personen ihr Recht auf Berichtigung und Löschung (Recht auf Vergessenwerden) ausüben?

Anfragen betroffener Personen (Art. 15 DS-GVO) und die Bearbeitung von Betroffenenrechten erfolgen zunächst durch den Verantwortlichen, an den die betroffene Person ihre Anfrage richtet. Das Thüringer Finanzministerium leistet im Einzelfall auf Anforderung der einsetzenden Behörde hierbei Unterstützung.

Löschbegehren und Berichtigungsanfragen hinsichtlich personenbezogener Daten (z. B.
Fehlerhafter Angaben in einem bereits gestellten Antrag) werden unverzüglich an die zuständige Behörde weitergeleitet. Die Bearbeitung des Anliegens erfolgt anschließend in dieser Behörde.

## Wie können betroffene Personen ihre Rechte auf Einschränkung oder Widerspruch der Verarbeitung ausüben?

Anfragen betroffener Personen (Art. 15 DS-GVO) und die Bearbeitung von Betroffenenrechten erfolgen zunächst durch den Verantwortlichen, an den die betroffene Person ihre Anfrage richtet. Das Thüringer Finanzministerium leistet im Einzelfall auf Anforderung der einsetzenden Behörde hierbei Unterstützung.

Aufforderungen zur Einschränkung der Verarbeitung und zum Widerspruch der Verarbeitung personenbezogener Daten werden unverzüglich an die zuständige Behörde weitergeleitet. Die Bearbeitung des Anliegens erfolgt anschließend in dieser Behörde.

## Sind die Verpflichtungen der Auftragsverarbeiter klar definiert und vertraglich geregelt?

Die Aufgaben der Auftragsverarbeiter IT.N und FJD AG sind in den Vereinbarungen zur Auftragsverarbeitung (Art. 28 (3) DS-GVO) definiert und geregelt.

## Soweit Datenübermittlungen in Länder außerhalb der Europäischen Union stattfinden, werden die Daten angemessen geschützt?

Zuständige Stelle

# Risiken

## Geplante oder bestehende Maßnahmen

### Logische Sicherheitsmaßnahme

#### Verschlüsselung

*Maßnahmen, die für die****Gewährleistung der Vertraulichkeit****der gespeicherten Daten (in der Datenbank, in unstrukturierten Dateien, Backups usw.) sowie das Verfahren zur Verwaltung der verwendeten kryptographischen Schlüssel (Erstellung, Speicherung, Änderung bei Verdacht auf Datengefährdung, Zugriffschutz usw.) implementiert sind.
Beschreiben Sie die für die Datenübermittlung verwendeten Verschlüsselungsverfahren (VPN, TLS usw.).*

Die Kommunikation zum Webserver ist mit SSL/TLS verschlüsselt.

#### Anonymisierung

*Beschreibung der Mechanismen der Anonymisierung, wie sie ausgestaltet sind und zu welchem Zweck sie umgesetzt werden und wie sie eine mögliche Reidentifikation verhindern. Beachten Sie den Unterschied zwischen Anonymisierung und Pseudonymisierung.*

Es findet keine Anonymisierung der Daten statt und ist auch nicht vorgesehen.

#### Datentrennung

*Die Implementierung einer Datentrennung trägt dazu bei, die Möglichkeit zu verringern, dass* *personenbezogene Daten verknüpft werden können und reduzieren so das Risiko eines unbefugten Zugriffs auf sämtliche gespeicherten personenbezogenen Daten.*

Die Datenbestände in ThAVEL werden nach Mandanten getrennt, so dass jede zuständige Stelle und jeder Betreiber einer eingebetteten App nur ihre eigenen Daten sehen kann.

#### Logische Zugriffskontrolle

*Beschreiben Sie die Definition und Zuweisung von Benutzerprofilen, Rollen und Rechten. Zudem ist es erforderlich, die verwendeten****Authentifizierungsmethoden****detailliert zu spezifizieren und gegebenenfalls die für Kennwörter geltenden Regeln anzugeben (Mindestlänge, obligatorische Struktur, Gültigkeitsdauer, Anzahl der erfolglosen Versuche bevor das Konto gesperrt wird, etc.).*

Der Zugriff auf ThAVEL und die zuständige Stelle erfolgt über Username und Passwort ohne Zweifaktorauthentifizierung. Das Rollenkonzept ist detailliert im Betriebshandbuch beschrieben. Es gibt Administratoren mit technischem Zugriff, zuständige Stellen für die inhaltliche Redaktion der Apps und Endkunden, die Anträge stellen.

#### Rückverfolgbarkeit (Protokollierung)

*Maßnahmen zur Sicherstellung der Revisionsfähigkeit von Verarbeitungsvorgängen, insbesondere Protokollierungs- und Auswertungsrichtlinien.*

Während des Betriebs von ThAVEL wird eine Logdatei geschrieben, Revisionssicherheit ist jedoch nicht gegeben. Eine ausführliche Beschreibung der Betriebsprotokolle ist sowohl im Betriebskonzept, als auch in der Steuerdatei: „log\_description.txt“ vorhanden.

#### Archivierung

*Beschreiben Sie die Aufbewahrungsrichtlinien sowie die Prozesse zur Verwaltung von Archiven, die personenbezogene Daten enthalten (Anlieferung von Daten, Speicherung, Zugriffsrechte, Aussonderung). Beschreiben Sie die Rollen und rechtlichen Grundlagen und Sicherheitsmaßnahmen der Archivierung. Falls erforderlich, beschreiben Sie die Regelungen zur* *Abgabe an staatliche Archive.*

Es erfolgt keine Archivierung in ThAVEL, Vorgänge werden nach 388 Tagen automatisch gelöscht. Dabei wird 360 Tage nach Erhebung der Daten eine Löschankündigung versandt, welche weitere 28 Tage später vollzogen wird.

Zuständige Stelle

#### Papierdokumentensicherheit

*Soweit Papierdokumente verarbeitet werden, sollte es entsprechende Richtlinien geben. Sie sollten beschreiben, wie Dokumente gedruckt, gelagert, vernichtet und übermittelt werden.*

Der Betrieb von ThAVEL erfolgt ausschließlich digital.

Zuständige Stelle.

#### Datenminimierung

*Der Umfang der Daten und damit die Sensibilität kann u.a. mit den folgenden Methoden reduziert werden: Filterung und Entfernung, Verringerung der Sensibilität durch Transformationen, Reduzierung des identifizierenden Merkmale der Daten, Aggregation von Daten, Beschränkung des Zugangs zu Daten.*

Die Ausgestaltung der Anträge und damit des erfassten Datenumfangs obliegt der jeweils zuständigen Stelle für einen Antrag. Typischerweise orientieren sich diese an den amtlichen Vordrucken.

### Physische Sicherheitsmaßnahme

#### Betriebssicherheit

*Richtlinien zur Begrenzung der Eintrittswahrscheinlichkeit hinsichtlich von Risiken bezüglich der Betriebsmittel (Dokumentation der Betriebsverfahren, Inventarisierung und Aktualisierung von Software und Hardware, Behebung von Sicherheitslücken, Duplizierung von Daten, Beschränkung des physischen Zugriffs auf Materialien usw.).*

Die allgemeinen Eigenschaften des Landesnetzes in dem die Server betrieben werden, sind den entsprechenden IT-Sicherheitskonzepten zu entnehmen, welche bei berechtigten Interesse auf Antrag im TFM eingesehen werden können.
Generell ist der physische Zugang zum Rechenzentrum durch zwei Ebenen  beschränkt.

#### Bekämpfung von Malware

*Maßnahmen zum Schutz des Zugangs zu öffentlichen (Internet-) oder unkontrollierten (Partner-) Netzwerken sowie Arbeitsplatzrechnern und Servern gegen bösartigen Code, der die* *Sicherheit der personenbezogenen Daten beeinträchtigen könnte.*

Malware wird durch technische Maßnahmen (Proxys, Firewalls, Virenscanner) abgefangen*.*

#### Arbeitsplatzverwaltung

*Maßnahmen, die ergriffen wurden, um zu verhindern, dass die Eigenschaften der Software (Betriebssysteme, Geschäftsanwendungen, Bürosoftware, Einstellungen usw.) dazu genutzt werden, personenbezogene Daten zu kompromittieren (Aktualisierungen, physischer Schutz und Zugriff, Arbeiten in einem gesicherten Netzwerkbereich, Integritätstest, Protokollierung usw.).*

Es handelt sich um eine Webanwendung, die hinter einem Application-Security-Gateway mit Content-Filtering betrieben wird. Dadurch werden gängige Angriffsszenarien neutralisiert.

Zuständige Stelle

#### Schutz des Internetauftritts

*Maßnahmen, um zu verhindern, dass die Eigenschaften von Websites zur Verletzung personenbezogener Daten missbraucht werden (allgemeine Sicherheitsrichtlinien, TLS-Verschlüsselung von Übermittlungen, Cookie-Richtlinien, Sicherheits-Audits usw.).*

Der Internetauftritt von ThAVEL wird durch Einsatz von technischen Maßnahmen (Application-Security-Gateway,Content Inspection , Maßnahmen gegen XSRF) geschützt. Passworte werden ausschließlich gehasht abgelegt.

#### Datensicherungen

*Vorhandensein einer Backup-Richtlinie, um die Verfügbarkeit und / oder Integrität von personenbezogenen Daten zu gewährleisten und gleichzeitig deren Vertraulichkeit zu schützen (Regelmäßigkeit der Backups, Verschlüsselung des Datenübertragung, Integritätstest usw.).*

Es erfolgen regelmäßige Datensicherungen gemäß Backup-Konzept. Zusätzliche Skripte stellen die Konsistenz der Daten sicher.
Ein Rücksicherungstest wird durchgeführt.

#### Hardware-/ Gerätewartung

*Richtlinien, die beschreiben, wie die physische Wartung und Sicherheit von Hardware durchgeführt wird, unter Angabe der möglichen Verwendung von Unterauftragsverarbeitern.
Geben Sie an, ob eine Fernwartung und unter welchen Vorkehrungen diese vorgesehen ist. Geben Sie an, wie mit fehlerhaften Geräten umgegangen wird.*

Die Hardware- und Gerätewartung erfolgt gemäß Leistungsscheinen der eingesetzten IT.N-Produkte.

#### Auftragsverarbeitungsvertrag

*Personenbezogene Daten, die an Auftragsverarbeiter übermittelt oder von diesen verwaltet werden, müssen ausreichende Garantien aufweisen. Hierzu sind vertragliche Regelungen erforderlich****Verwenden Sie nur Auftragsverarbeiter mit ausreichender Zuverlässigkeit****(insbesondere in Bezug auf Fachwissen, Zuverlässigkeit und Ressourcen). Fordern Sie die Sicherheitsrichtlinie für das Informationssystem des Anbieters ein.
Ergreifen und dokumentieren Sie die Maßnahmen (Sicherheitsaudits, Besuche von Einrichtungen usw.), um****die Wirksamkeit der Garantien zu gewährleisten, die der Auftragsverarbeiter*** *im Hinblick auf den Datenschutz bietet. Diese Garantien umfassen:
- die Verschlüsselung von Daten entsprechend ihrer Sensibilität oder, falls dies nicht der Fall ist, die Existenz von Verfahren, die gewährleisten, dass das Dienstleistungsunternehmen keinen Zugang zu den ihm anvertrauten Daten hat,
- die Verschlüsselung von Übertragungen von Daten (z.B.: HTTPS-Verbindung, VPN, etc.)
- Garantien in Bezug auf Netzwerkschutz, Rückverfolgbarkeit (Protokolle, Audits), Autorisierungsverwaltung, Authentifizierung, usw.****Bereitstellung eines Vertrags mit dem Auftragsverarbeiter****, der den Zweck, die Dauer, den Zweck der Verarbeitung und die Verpflichtungen der Parteien definiert. Stellen Sie sicher, dass er insbesondere Bestimmungen enthält, die Folgendes enthalten:
- ihre Verpflichtung zur Vertraulichkeit personenbezogener Daten, die ihr anvertraut sind
- Mindestanforderungen an die Benutzerauthentifizierung
- die Bedingungen für die Rückgabe und / oder Vernichtung / Löschung von Daten am Ende des Vertrags
- die Regeln der Handhabung und die Benachrichtigung bei Datenschutzvorfällen. Diese sollten im Falle einer Sicherheitsverletzung oder eines Sicherheitsvorfalls Informationen des für die Verarbeitung Verantwortlichen enthalten, und dies im Falle einer Verletzung des Schutzes personenbezogener Daten so schnell wie möglich.
- Bei Einsatz eines Cloud-Anbieters:
1. Benennen Sie eindeutig die Daten und die Verarbeitung, die in die Cloud ausgelagert werden;
2. Definition eigener technischer und rechtlicher Sicherheitsanforderungen;
3. Führen Sie eine Risikostudie durch, um geeignete Sicherheitsmaßnahmen zu ermitteln;
4. Identifizieren des relevante Art der Cloud für die beabsichtigte Verarbeitung;
5. Wählen Sie einen Anbieter mit ausreichenden Garantien;
6. Überprüfen Sie die interne Sicherheitsrichtlinie;
7. Überwachen Sie Änderungen während der Laufzeit.*

Für den Betrieb von ThAVEL existieren Auftragsverarbeitungen mit IT.Niedersachsen als Betreiber und mit der Firma FJD AG als Entwickler von ThAVEL (Stand: 12/2020). Durch die Vereinbarung nach Art. 26 DS-GVO welche die Aufgabenverteilung der gemeinsam für die Nutzung von ThAVEL Verantwortlichen wird das Thüringer Finanzministerium als das für E-Government und IT zuständige Ministerium ermächtigt, stellvertretend für den Kreis der gemeinsam Verantwortlichen Auftragsverarbeitungsverhältnisse abzuschließen.

#### Netzwerksicherheit

*Je nach Art des Netzwerks, auf dem die Verarbeitung ausgeführt wird (isoliert, privat oder Internet), muss der Verantwortliche angemessene Schutzsysteme installieren: Firewalls, Intrusion Detection Systeme oder andere aktive oder passive Geräte, die für die Sicherstellung der Netzwerksicherheit verwendet werden.*

Gemäß Landesnetz IT-Sicherheitskonzept des Betreibers (IT.N).

#### Zugangskontrolle

*Vorhandensein einer physischen Zugangskontrolle zu den Räumlichkeiten, in denen die Verarbeitung durchgeführt wird (Zonierung, Begleitung der Besucher, Tragen von Abzeichen, verschlossene Türen usw.) - Geben Sie an, ob bei einem Einbruch Alarm ausgelöst werden kann.*

Der Zutritt zum Rechenzentrum, in welchem ThAVEL betrieben wird, ist nur für autorisiertes Personal möglich. Näheres dazu findet sich im IT-Siko des Rechenzentrums von IT.N.

Zuarbeit Zuständige Stelle

#### Überwachen der Netzwerkaktivität

*Vorhandensein von Maßnahmen zur Überwachung der Netzwerkaktivitäten (in drahtlosen wie drahtgebundenen Netzen) in Echtzeit, um Vorfälle in Bezug auf personenbezogene Daten frühzeitig zu erkennen und verwertbare Informationen zu deren Untersuchung oder zur Bereitstellung von Nachweisen zu liefern.*

Es bestehen technische Systeme (Security Operations Center, Intrusion Detection System) welche das Netzwerk auf verdächtige Aktivitäten überwachen.

#### Hardware-Sicherheit

*Maßnahmen, die ergriffen wurden, um die Möglichkeit zu verringern, dass die eingesetzten Systeme (Server, Workstations, Laptops, Peripheriegeräte, Kommunikationsgeräte, Wechselmedien usw.) zur Beschädigung personenbezogener Daten verwendet werden (Inventarisierung, Trennung, physische Redundanz, Zugangsbeschränkungen usw.).*

Einsatz von redundanten Virtuellen Maschinen limitieren Ausfälle der Hardware.

#### Vermeidung von Risikoquellen

*Vorhandensein von Maßnahmen zur Vermeidung von menschlichen oder nichtmenschlichen Risikoquellen für den Schutz personenbezogener Daten (gefährliche Produkte, gefährliche geografische Gebiete, Datenübermittlung außerhalb der EU usw.).*

Es sind keine konkreten Risikoquellen bekannt. Somit wurden keine konkreten Maßnahmen getroffen.

Zuständige Stelle

#### Schutz vor nichtmenschlichen Risikoquellen

*Vorhandensein von Maßnahmen zur Verringerung oder Vermeidung von Risiken in Verbindung mit nichtmenschlichen Quellen (Klimaphänomene, Feuer, Wasserschäden, interne oder externe Unfälle, Tiere usw.), die die Sicherheit personenbezogener Daten beeinträchtigen könnten (Präventivmaßnahmen, Erkennung, Schutz usw.).*

Im IT-Sicherheitskonzept sind technisch-organisatorische Maßnahmen festgelegt. Dazu gehören der Einsatz eines Application Security Gateway, um automatisierte Angriffe aus dem Netz abzuwehren und der Betrieb im sicheren Rechenzentrum des IT.Niedersachsen. Auch der Einsatz von SSL zählt zu diesen Maßnahmen. Eine Georedundanz der Rechenzentren ist derzeit (Stand: 11/2020) nicht gegeben, Der künftige Betrieb von ThAVEL soll jedoch in georedundanten Rechenzentren stattfinden.

Zuständige Stelle

### Organisationsmaßnahme

#### Datenschutzorganisation

*Vorhandensein einer Organisationseinheit, die in der Lage ist, den Schutz personenbezogener Daten innerhalb der Organisation zu steuern und zu kontrollieren (Benennung eines DSB, Einrichtung eines Teams für das Datenschutzmanagement usw.).*

Durch den Betreiber von ThAVEL wurde im IT-Sicherheitskonzept eine Analyse durchgeführt und daraus technisch-organisatorische Maßnahmen (TOMs) abgeleitet. Daraus resultierte ein Umsetzungsplan, der von einem Audit mit Penetrationstest auf Umsetzung geprüft wurde.

Der Softwarehersteller hat für das Datenschutzmanagement eine externe Firma beauftragt.

Zuständige Stelle

#### Datenschutzrichtlinien

*Der für die Verarbeitung Verantwortliche muss über eine Dokumentation verfügen, in der die Zielgruppen und Regeln für die Umsetzung des "Datenschutzes" festgelegt sind (Aktionsplan, regelmäßige Überarbeitung der Datenschutzrichtlinien usw.).*

Die Datenschutzrichtlinien des Betreibers von ThAVEL sind in dem IT-Sicherheitskonzepts von IT.N geregelt, welche im TFM vorliegt und bei berechtigten Interesse auf Antrag in den Räumlichkeiten des TFM eingesehen werden kann.

Zuständige Stelle

#### Management von Datenschutzrisiken

*Vorhandene Regelung und Verfahren zum Management der Risiken, die die Verarbeitungen der Organisation für die Rechte und Freiheiten der betroffenen Personen darstellen (Identifizierung der Verarbeitungsverfahren, der verarbeitenden Daten, Betriebsmittel, Risikobewertung, Ermittlung bestehender oder geplanter Maßnahmen usw.).*

Zuständige Stelle

#### Integration des Schutzes der Privatsphäre in Projekte

*Vorhandene Verfahren zur Beschreibung der Methoden zur Berücksichtigung des Schutzes* *personenbezogener Daten bei jeder neuen Verarbeitung (Zertifizierungen, Normen, Risikomanagement für die betreffende Person nach der CNIL-Methode oder eine interne Methode usw.).*

Zuständige Stelle

#### Umgang mit Datenschutzverletzungen

*Existenz einer operativen Einheit zur Aufdeckung und Behandlung von Ereignissen, die die Freiheiten und die Privatsphäre der betroffenen Personen beeinträchtigen können (Definition von Verantwortlichkeiten, Reaktionsplan, Charakterisierung von Verstößen, etc.).*

Zuständige Stelle

#### Sensibilisierungsmaßnahmen

*Vorhandene Regelungen zur Schulung und****Sensibilisierung****von (neuen) Mitarbeitern bei Antritt ihrer (neuen) Funktion sowie für Personen, die Zugriff auf personenbezogene Daten hatten beim Ausscheiden aus der Organisation.*

Zuständige Stelle

#### Sicherheitsmaßnahmen und -regelungen für Dritte

*Vorliegen von Regelungen und Maßnahmen zur Verringerung der Risiken, die der legitime Zugang zu Daten durch Dritte für die Freiheiten und die Privatsphäre der betroffenen Personen darstellen kann (Festlegung der Dritten, Auftragsverarbeitungsvertrag, Verpflichtungen, Binding Corporate Rules usw.).*

Der Zugriff des ist nur über eine genau zugeschnittene Verwaltungskonsole möglich.

Zuständige Stelle

#### Überwachung der Datenschutzmaßnahmen

*Vorhandensein von Maßnahmen, um einen globalen und aktuellen Überblick über den Stand des Datenschutzes und die Einhaltung der DS-GVO zu erhalten (Überprüfung der Einhaltung* *von Verarbeitungen, Zielen und Indikatoren, Verantwortlichkeiten usw.).*

Zuständige Stelle

## Unrechtmäßiger Zugriff auf Daten

### Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

Zuständige Stelle

### Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

Zuständige Stelle

### Was sind die Risikoquellen?

Zuständige Stelle

### Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos (Unrechtmäßiger Zugriff auf Daten) bei?

Zuständige Stelle

### Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Zuständige Stelle

### Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplante Maßnahmen?

Zuständige Stelle

## Unerwünschte Veränderung von Daten

### Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

Zuständige Stelle

### Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

Zuständige Stelle

### Was sind die Risikoquellen?

Zuständige Stelle

### Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos (Unerwünschte Veränderung von Daten) bei?

Zuständige Stelle

### Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Zuständige Stelle

### Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplante Maßnahmen?

Zuständige Stelle

## Datenverlust

### Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

Zuständige Stelle

### Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

Zuständige Stelle

### Was sind die Risikoquellen?

Zuständige Stelle

### Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos (Datenverlust) bei?

Zuständige Stelle

### Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Zuständige Stelle

### Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplante Maßnahmen?

Zuständige Stelle