



Envoria - Technische und organisatorische Maßnahmen

The background of the top half of the page is a vibrant, stylized illustration of a landscape. It features rolling green hills, a winding blue river, and distant mountains under a bright blue sky with wispy clouds. In the foreground, there are dark green silhouettes of trees and bushes. Several wind turbines are visible on the left side, and a large electricity pylon stands on the right side.

– Nach Artikel 32 DSGVO –

Inhaltsverzeichnis

1. Einleitung	3
2. Die SaaS Lösungen	3
3. Technische und organisatorische Maßnahmen	3
a. Zutrittskontrollen	3
b. Zugangskontrollen	4
c. Zugriffskontrollen	4
d. Trennungskontrollen	5
e. Pseudonymisierung und Verschlüsselung	5
f. Weitergabekontrollen	6
g. Eingabekontrollen	6
h. Verfügbarkeitskontrollen	6
i. Belastbarkeit	7
j. Überprüfung, Bewertung und Evaluierung	7
k. Auftragskontrollen	8

1. Einleitung

Es wird vom Auftragnehmer ein für die konkrete Auftragsverarbeitung angemessenes Schutzniveau gewährleistet. Dies wird wie folgt beschrieben:

Die weisungsgemäße Auftragsdatenverarbeitung ist gewährleistet durch die technisch / organisatorische Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer. Eine Auftragsdatenverarbeitung erfolgt nur in Ausnahmefällen durch Dienstleistungen für Systemeinrichtung, Betreuung, Schulung, Programmierung oder zum Nachvollziehen von Programmfunktionen.

2. Die SaaS Lösungen

Für den Betrieb der Cloud-Infrastruktur greift Envoria auf etablierte Anbieter aus dem Bereich Rechenzentren und Cloud-Services zurück. Die Hosting-Umgebung wird dabei innerhalb moderner, cloudbasierter Rechenzentren betrieben, die bei Nutzung von Envoria durch Exoscale und bei Nutzung von Envoria Lease Accounting durch Hetzner Online GmbH bereitgestellt werden. Diese Infrastruktur befindet sich innerhalb der Europäischen Union oder in Staaten mit entsprechendem Angemessenheitsbeschluss der EU-Kommission.

Weitere Details zu den Sicherheitsstandards und -maßnahmen der Cloud-Anbieter, können auf der offiziellen Sicherheitsseite von [Exoscale](#) und [Hetzner Online GmbH](#) eingesehen werden.

3. Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i. S. d. Art. 32 DS-GVO. Die Wirksamkeit dieser Maßnahmen wird regelmäßig überprüft, bewertet und weiterentwickelt.

a. Zutrittskontrollen

Maßnahmen, die verhindern, dass Unbefugte Zutritt bekommen, in/mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Technische Maßnahmen	Organisatorische Maßnahmen
→ Die Geschäftsräume des Auftragnehmers befinden sich in einem Bürogebäude. Die Eingangstür ist durch ein Schließsystem gesichert. → Zugang zum Rechenzentrum wird protokolliert, überwacht und zurückverfolgt	→ Einführung von Zugangsberechtigungen für Mitarbeiter und Dritte sowie entsprechende Dokumentation → Der Zutritt zum Gebäude wird durch einen Empfang Personell belegt → Verpflichtende Besucheranmeldung → Besucher nur in Begleitung durch Mitarbeiter → Wachpersonal außerhalb der gewöhnlichen Betriebszeiten → Es erfolgte eine sorgfältige Auswahl von Reinigungspersonal → Unverzügliche Sperrung von Zutrittsberechtigungen bei Ausscheiden von Mitarbeitern oder Dienstleistungen

b. Zugangskontrollen

Maßnahmen, die verhindern, dass Unbefugte Datenverarbeitungssysteme nutzen können.

Technische Maßnahmen	Organisatorische Maßnahmen
→ Physische Löschung von Datenträgern vor Wiederverwendung → Login mit Benutzername + Passwort + ggf. 2FA → Login mit biometrischen Daten → Automatische Desktopsperre → Festplatten-/Systemverschlüsselung mobiler Endgeräte	→ Erstellen eines Berechtigungskonzepts durch Systemadministrator → Passwortrichtlinie inkl. Passwortlänge, Passwortkomplexität → Sichere Aufbewahrung von Datenträgern → Ordnungsgemäße Vernichtung von Datenträgern → Verwaltung von Benutzerberechtigungen → Erstellen von Benutzerprofilen → Richtlinie für sichere Passwörter → Richtlinie zur Löschung und Vernichtung von Daten → Richtlinie zu Clear Desk und Clear Screen → Anleitung zur Manuellen Desktop Sperre → Unverzügliche Sperrung von Benutzerkonten bei Ausscheiden von Mitarbeitern

c. Zugriffskontrollen

Maßnahmen, die sicherstellen, dass Berechtigte nur Zugriff auf personenbezogene Daten haben, für welche eine dienstliche Notwendigkeit besteht.

Technische Maßnahmen	Organisatorische Maßnahmen
→ Der Zugriff auf die Daten wird durch differenzierte Berechtigungen geschützt. → Authentifikation mit Benutzername/Passwort → Automatische Logout bei längerer Nichtnutzung, Wiederaufnahme nach Identifizierung und Passworteingabe des Nutzers → Einsatz von Anti-Viren-Software, einer Software-Firewall und ggfs. von VPN-Technologie → Protokollierung von Zugriffen	→ Zuordnung von Benutzerrechten, Benutzerprofilen und durch Passwortvergabe → Einsatz von Berechtigungskonzepten → Vergabe von Zugriffsrechten nach dem Need-to-Know-Prinzip

d. Trennungskontrollen

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
→ Physisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern → Trennung von Produktiv- und Testsystemen	→ Erstellung eines Berechtigungskonzepts → Steuerung über Berechtigungskonzept → Logische Mandanten-Trennung der Kundendaten

e. Pseudonymisierung und Verschlüsselung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen keiner betroffenen Person zugeordnet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
→ Verschlüsselung von Festplatten mit Windows Standardtools. → Die Übertragung von Daten über das Internet erfolgt immer verschlüsselt mit dem aktuell gängigen technischen Verfahren → Verschlüsselung von Backups	→ Eine Pseudonymisierung kommt nicht zum Tragen, da die Daten im Original gebraucht werden, um einen Fehler in der Softwareanwendung/Softwareanwendung unter realistischen Bedingungen nachvollziehen zu können. → Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren.

f. Weitergabekontrollen

Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der Übermittlung oder der Speicherung oder beim Transport auf externen Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
→ Einrichtung von Standleitungen bzw. VPN-Tunneln nur zusammen mit dem Auftraggeber → E-Mail-Verschlüsselung → Protokollierung von Zugriffen → Bereitstellung über verschlüsselte Verbindungen wie https	→ Dokumentation der Datenempfänger sowie der Dauer der geplanten Löschfristen → Sorgfalt bei Auswahl von Transportwegen → Sorgfalt bei Auswahl von Personal → Vertraulichkeits-/Geheimhaltungsvereinbarung mit externen Empfängern personenbezogener Daten

g. Eingabekontrollen

Maßnahmen, die es erlauben, nachträglich zu überprüfen, ob personenbezogene Daten, welche eingegeben wurden, auch den angelieferten Daten entsprechen. Die Eingabe wird über eine Protokollierung auf Ebene des Systems oder der Anwendung kontrolliert.

Technische Maßnahmen	Organisatorische Maßnahmen
→ Nur personalisierte Benutzerkonten im Einsatz – keine generischen → Serverprotokollierung (Anmeldungen, Fehlermeldungen), Anwendungsprotokollierung (Anmeldungen, Änderung von Inhalten/Werten, Fehlermeldungen)	→ Übersicht, mit welchen Programmen welche Daten verarbeitet werden → Vergabe von Rechten zur Eingabe, Veränderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

h. Verfügbarkeitskontrollen

Maßnahmen zur Wahrung der Verfügbarkeit sollen sicherstellen, dass die verarbeiteten personenbezogenen Daten auch nach einem Zwischenfall weiterhin zur Verfügung stehen, um den Betrieb wieder aufzunehmen.

Technische Maßnahmen	Organisatorische Maßnahmen
→ Feuer- und Rauchmeldeanlage im Gebäude → Aufbewahrung der Sicherungsmedien an 2 geographisch unterschiedlichen Standorten	→ Backup & Recovery-Konzept vorhanden → Regelmäßige Kontrollen der Sicherungsvorgänge → Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse → Dokumentierter BCM-Prozess

i. Belastbarkeit

Maßnahmen, die die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung gewährleisten, d. h. deren Fähigkeit, auch bei hoher Last, Störungen oder Angriffen stabil und funktionsfähig zu bleiben.

Technische Maßnahmen	Organisatorische Maßnahmen
→ Redundante IT-Infrastruktur → Automatische Skalierung der Ressourcen	→ Dokumentierter BCM-Prozess

j. Überprüfung, Bewertung und Evaluierung

Maßnahmen, die die fortlaufende Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sicherstellen.

Technische Maßnahmen	Organisatorische Maßnahmen
→ Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	→ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird regelmäßig o. bei Bedarf durchgeführt → Besteller Datenschutzbeauftragter → Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet → Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich → Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach → Dokumentation von Sicherheitsvorfällen und Datenpannen → Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind → Dokumentierter Prozess zur Meldung von Datenschutzverletzungen an die Aufsichtsbehörde und betroffene Personen → Regelmäßige Überprüfungen der technischen und organisatorischen Maßnahmen

k. Auftragskontrollen

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
	→ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation → Auswahl des Auftragnehmers unter Sorgfalt Gesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit) → Abschluss der notwendigen Vereinbarungen zur Auftragsverarbeitung → Schriftliche Weisung an den Auftragnehmer → Bestätigung zur Einhaltung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis → Verpflichtung zur Bestellung eines DSB durch den Auftragnehmer bei Vorliegen einer Bestellpflicht → Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer → Regelung zum Einsatz weiterer Subunternehmer → Sicherstellung der Vernichtung o. Rückgabe von Daten nach Beendigung des Auftrags → Regelmäßige Kontrolle der eingesetzten Auftragsverarbeiter/Subunternehmer hinsichtlich der Einhaltung der vereinbarten Sicherheitsmaßnahmen