Technische und Organisatorische Maßnahmen (TOM)

Letzte Aktualisierung: August 2026

1. Zutrittskontrolle

1.1 Büroräume

- Enneo ist eine vollständig virtuelle Firma ohne Büroräume, daher entfällt die Notwendigkeit einer baulichen Zutrittskontrolle
- Etwaige künftige Büroräume werden über angemessene Sicherheitsvorkehrungen verfügen, insb. über maschinelle Zutrittskontrollsysteme

1.2 Rechnerräume ("Closed Shop" - Betrieb) über unseren AV Hetzner

- Elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um den gesamten Datacenter-Park
- Dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
- Der Zutritt ist nur in Begleitung eines Hetzner Online GmbH Mitarbeiters möglich

2. Zugangskontrolle

2.1 Zugangskontrollmaßnahmen

- Es liegt eine zentrale Beschreibung aller Zugänge zu gesicherten Daten vor.
- Der Zugang zu personenbezogenen Daten benötigt zwei Faktoren (2FA), z.B. Login/Passwort und One-Time-Passwort (OTP), oder Zertifikat und Passphrase.
- Die Komplexität von Passwörtern und PINs unterliegt Mindestanforderungen, die dem aktuellen Stand der Technik entsprechen.
- Der Umgang mit Passwörtern (z.B. Verbot der Weitergabe, Aufbewahrung) ist schriftlich geregelt.

2.2 Zugangssicherung

- Enneo’s Sicherheitskonzept basiert auf der „Zero Trust Sicherheitsarchitektur“[1]. Das Zero Trust-Modell geht davon aus, dass nichts sicher ist – auch nicht hinter der Firmenfirewall. Deshalb werden alle Anforderungen so überprüft, als kämen sie aus einem offen zugänglichen Netzwerk.
- Dennoch wird zusätzlich sichergestellt, dass:
- Benutzer nur Zugang zu den Netzdiensten bekommen, zu deren Nutzung sie ausdrücklich befugt sind.
- Externe Zugänge zum Netzwerk nur über eine gesicherte Verbindung (z.B. Zertifikat) hergestellt werden können.
- Nur berechtigte Personen logischen Zugang zu den Netzwerkkomponenten haben.
- Für Anwendungen, die aus dem Internet zugänglich sind, eine mehrstufige IT-Architektur sowie eine demilitarisierte Zone (DMZ) existieren. Netzwerksegmente sind nach ihrem

Schutzbedarf auf verschiedenen Ebenen voneinander getrennt, um den Datenverkehr zwischen unterschiedlich schutzbedürftigen Segmenten zu verhindern.

- Die Verwendung externer physischer Schnittstellen (bspw. USB, DVD) ist im Grundsatz untersagt.

3. Zugriffskontrolle

3.1 Zugriffsschutzmaßnahmen

- Zu jeder Zeit ist bekannt, welcher Mitarbeiter welchen Zugriff auf geschützte Daten hat. Der Status ist dokumentiert und wird stets aktualisiert.
- Der Zugang zu personenbezogenen Daten benötigt zwei Faktoren (2FA), z.B. Login/Passwort und One-Time-Passwort (OTP), oder Zertifikat und Passphrase.
- Ein Berechtigungskonzept regelt die Vergabe und den Entzug von Rechten. Nur ausdrücklich befugte Personen besitzen Zutritts-, Zugangs- und Zugriffsberechtigungen für die für die Leistungserbringung relevanten Ressourcen.
- Es existiert ein Validierungsprozess des Berechtigungsprozesses sowie der vergebenen Berechtigungen.
- Jegliche Veränderungen an den Berechtigungen werden revisionssicher dokumentiert, sodass nachvollziehbar ist, welche Berechtigungen zu welchem Zeitpunkt für welche Person eingerichtet wurden.
- Bei Ausscheiden eines Mitarbeiters ist sicherzustellen, dass die Zugänge zu den Systemen in angemessenem Zeitraum gesperrt werden, spätestens jedoch nach 5 Werktagen.
- Die Nutzer stellen sicher, dass ihre DV-Ausstattung ausreichend geschützt ist, wenn sie unbeaufsichtigt ist.
- Der Grundsatz des "aufgeräumten Schreibtischs" und des "leeren Bildschirms" wird aktiv umgesetzt.
- Es wird von der Verschlüsselung der Daten auf Dateisystem- oder Datenbankebene entsprechend der BSI Verschlüsselungsempfehlungen Gebrauch gemacht („Encryption at Rest“).

3.2 Sichere Entsorgung von Datenträgern und Dokumenten

Die Erstellung von physischen Datenträgern und Dokumenten (Papier) mit vertraulichen Daten ist im Grundsatz untersagt. Entsprechend entfallen Maßnahmen zur sicheren Entsorgung. Obige Regelung gilt nicht für Auftragsverarbeiter, welche angemessene Sicherheitsniveaus für die Entsorgung von Datenträgern und Dokumenten vorzuweisen haben, z. B. nach DIN 66399.

4. Weitergabekontrolle

4.1 Verpflichtung der Mitarbeiter auf das Datengeheimnis

- Alle Personen, die personenbezogene Daten automatisiert verarbeiten, sind auf das Datengeheimnis verpflichtet.
- Neue Mitarbeiter erhalten Informationen zum Datenschutz bei dem Umgang mit personenbezogenen Daten.
- Allen Beteiligten sind die Belange der Datensicherheit und des Datenschutzes bekannt.
- Personen, die personenbezogene Daten erheben, verarbeiten oder nutzen, sind durch Datenschutzschulungen auf datenschutzgerechtes Verhalten am Arbeitsplatz unterrichtet.

- Es gibt ausdrückliche Regelungen für die Behandlung ausscheidender, insbesondere gekündigter Mitarbeiter.

4.2 Richtlinie und Verfahren zur Klassifizierung von Daten

- Es gibt ein unternehmensweit gültiges Schema für die Klassifizierung von Daten.
- Das unternehmensweit gültige Verfahren zum Umgang mit klassifizierten Daten wird praktisch umgesetzt.

4.3 Physische Datenübergabe

- Das Unternehmen stellt sicher, dass Daten nur an die vom Auftraggeber festgelegten oder der Zweckbestimmung nach richtigen Adressaten übermittelt werden.
- Physische Datenträger sind per Arbeitsanweisung nicht im Einsatz.

4.4 Elektronische Datenübermittlung

- Das Unternehmen führt eine Übersicht/Liste über diejenigen Stellen, an denen Übermittlungen programmgesteuert stattfinden können.
- Eine Dokumentation der eingesetzten Programme für die automatisiert ausgelöste Übermittlung ist vorhanden.
- Die elektronische Übermittlung personenbezogener Daten wird durch Aufzeichnung des beteiligten Verfahrens, Empfänger, Daten, Datum und Uhrzeit revisionssicher protokolliert.
- Die Datenübermittlung erfolgt unter Einsatz geeigneter und angemessener Verschlüsselungstechniken.

4.5 Anonymisierung / Pseudonymisierung

- Bei der Weitergabe macht das Unternehmen von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch.
- Bei der Einrichtung einer Pseudonymisierung von Dokumentationsdaten ist sichergestellt, dass das Pseudonym bei dem Empfänger nicht wieder mit dem Klarnamen zusammengeführt werden kann.

5. Eingabekontrolle

5.1 Protokolle

- Es existiert ein Protokollierungskonzept, das Art, Inhalt und Umfang der Protokollierung festlegt und Incidentparameter in Protokollen beschreibt.
- Protokolle zeigen auf Benutzerebene, welche Anwendungen oder Dienste ein bestimmter Benutzer in einem definierten Zeitraum genutzt hat.
- Die zur Auswertung von Eingabeprotokollen genutzten Programme und Hilfsmittel sind dokumentiert. Gleiches gilt für die verwendeten Filterkriterien.
- Protokolldaten zur Eingabekontrolle sind gegen unbefugte Einsicht oder Manipulation geschützt.
- Für Protokolldateien zur Eingabekontrolle gelten die Löschfristen gemäß AVV Ziffer 1.2.
- Die Daten zur Eingabekontrolle unterliegen einer strengen Zweckbindung und werden nur für Zwecke der Datenschutzkontrolle ausgewertet und genutzt. Es erfolgt keine anlasslose Verhaltens- und Leistungskontrolle der Mitarbeiter über die Auswertung der Protokolldateien.

- Eine Betriebsrichtlinie / Policy ist vorhanden, welche die Vorgehensweise zur Auswertung von Protokolldaten bei einem Verdacht auf Sicherheitsverstöße, oder nach Sicherheitsverstößen, enthält.
- Enneo prüft stichprobenartig die Einhaltung der Richtlinien zur Protokollierung, führt regelmäßige Datenschutzaudits sowie anlass- und turnusbezogen Mitarbeiterschulungen durch.

5.2 Schwachstellenmanagement und Änderungsprozess

- Enneo führt regelmäßige automatisierte Schwachstellen-Scans der produktiven Infrastruktur durch.
- Enneo lässt die produktive Infrastruktur mindestens jährlich sowie nach wesentlichen Architekturänderungen durch einen externen Dienstleister einem Penetrationstest unterziehen.
- Änderungen an produktiven Systemen unterliegen einem dokumentierten Change-Management-Prozess einschließlich Vorab-Prüfung, Freigabe und Nachvollziehbarkeit der Änderung.
- Datenkategorien und Systeme sind gemäß dem unternehmensweiten Klassifizierungsschema (siehe Ziffer 4.2) eingestuft; die Klassifizierung bestimmt das anzuwendende Schutzniveau.

6. Auftragskontrolle

6.1 Datenschutzbeauftragter

Datenschutzbeauftragter (Artikel 37 bis 39 DS-GVO + nationales Recht). Sobald nach Artikel 37 DS-GVO bzw. Artikel 38 BDSG vorgeschrieben, benennt enneo einen Datenschutzbeauftragten. Bis zu diesem Zeitpunkt unterhält enneo die Funktions-Kontaktstelle datenschutz@enneo.ai für datenschutzrechtliche Anfragen und Meldungen. Für den Datenschutzbeauftragten gilt, sobald bestellt:

- Der Datenschutzbeauftragte wird in Ausübung seiner Aufgaben von niemandem angeleitet (Art. 38 Abs. 3 DS-GVO) und ist unmittelbar der obersten Managementebene berichtspflichtig, ohne ihr in der betrieblichen Organisation unterstellt zu sein.
- Enneo stellt sicher, dass keine Interessenkonflikte zwischen der Funktion des Datenschutzbeauftragten und etwaigen weiteren Aufgaben derselben Person bestehen (Art. 38 Abs. 6 DS-GVO); insbesondere ist ein Datenschutzbeauftragter, der zugleich Geschäftsführungsaufgaben wahrnimmt, von Entscheidungen über Zwecke und Mittel der Verarbeitung ausgeschlossen.
- Der Datenschutzbeauftragte verfügt über die für das Unternehmen erforderliche Fachkunde und Zuverlässigkeit.
- Der oder die Datenschutzbeauftragte ist schriftlich bestellt worden; die Bestellungsurkunde kann im Rahmen eines Kundenaudits eingesehen werden.
- Die Geschäftsführung unterstützt den Datenschutzbeauftragten und stellt die hierfür erforderlichen Ressourcen bereit.
- Der Datenschutzbeauftragte wird bei der Planung neuer Verfahren oder der Änderung bestehender Verfahren rechtzeitig informiert und einbezogen und gestaltet die Verfahrenskonzeption aktiv mit.

6.2 Vertragliche Verpflichtung

- Alle Auftragnehmer einer Auftragsverarbeitung sind vertraglich durch den Auftraggeber gebunden.

- Der schriftliche Auftrag erfüllt den Regelungskatalog von Artikel 28 Abs. 3 DS-GVO.

6.3 Auswahl des Auftragnehmers

- Dem Auftraggeber lagen vor der Beauftragung aussagekräftige Informationen über den Datenschutz und die technischen und organisatorischen Maßnahmen bei dem Auftragnehmer vor.
- Die Entscheidung und die Begründung für die Auswahl des Auftragnehmers wurde von dem Unternehmen dokumentiert.
- Das Unternehmen überzeugt sich vor Beginn der Verarbeitung von der Einhaltung des Datenschutzes bei Auftragnehmern in den Bereichen, die nicht durch Zertifikate nachgewiesen werden, und kontrolliert Auftragnehmer sodann regelmäßig.

6.4 Weisungen

- Der Auftraggeber benennt gegenüber dem Auftragnehmer die weisungsberechtigten Personen.
- Der Auftragnehmer benennt dem Auftraggeber als befugten Weisungsempfänger Dr. Richard Lohwasser (richard@enneo.ai) sowie die Funktions-Kontaktstelle datenschutz@enneo.ai.
- Weisungen erfolgen schriftlich.

6.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Ein unternehmensweites Datenschutz- und Risikomanagementsystem ist etabliert, welches die Anforderungen der EU-DSGVO erfüllt.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).

7. Verfügbarkeitskontrolle

7.1 Sicherheitsmaßnahmen

- Monitoring aller relevanten Server
- Dauerhaft aktiver DDoS-Schutz
- Einsatz unterbrechungsfreier Stromversorgung mit Netzersatzanlage sowie physischer Zugangs- und Zutrittskontrollen bei den Rechenzentrumsbetreibern Hetzner Online GmbH und (für Backups) aixit GmbH gemäß deren jeweiligen Sicherheitskonzepten
- Einsatz von Festplattenspiegelung
- Der Wiederanlauf der IT-Systeme nach dem Katastrophenfall erfolgt in kurzer Zeit, da Infrastruktur softwareseitig spezifiziert ist („Infrastructure-as-code“). Die Recovery Time Objective (RTO) und Recovery Point Objective (RPO) je Service Level ergeben sich aus Abschnitt 3.1 der Anlage „Service Level Agreement“.
- Enneo führt ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO, das dem Auftraggeber auf Anfrage zur Verfügung gestellt wird.

7.2 Backup-Konzept

- Alle Daten werden mindestens täglich gesichert. Dabei werden die Backup-Daten verschlüsselt abgelegt.
- Die Rücksicherung und Integrität vorhandener Backups wird regelmäßig getestet.

- Aufbewahrungsfristen für Backups ergeben sich aus Abschnitt 3.1 der Anlage „Service Level Agreement“.

8. Trennungskontrolle

8.1 Mandantenfähigkeit

- Beim Einsatz von Mehrmandantensystemen erfolgt eine ausreichende Mandantentrennung. Dabei sind Daten der verschiedenen Kunden untereinander nicht einsehbar und nicht veränderbar. Auch sind keine Rückschlüsse auf die jeweiligen Kunden möglich. Der Auftraggeber wird über den Einsatz sowie die Funktionsweise von Mehrmandantensystemen informiert.
- Im Falle eines Ermittlungsverfahrens (Polizei, Steuerfahndung o.ä.) prüft enneo die Rechtmäßigkeit der behördlichen Maßnahme, beschränkt deren Umsetzung auf das rechtlich Gebotene und informiert den Auftraggeber unverzüglich, soweit dies rechtlich zulässig ist; eine Pfändung oder Beschlagnahme nach AVV Ziffer 6.8 bleibt hiervon unberührt.
- Sicherheitsvorfälle im Mehrmandantensystem (jedweder Art), mit Auswirkungen auf den ausgelagerten Bereich des Auftraggebers, werden diesem unverzüglich zur Kenntnis gebracht.

8.2 Trennung von Umgebungen

- Office-, Entwicklungs-/Test- und Produktivsysteme werden in logisch klar voneinander getrennten Netzsegmenten betrieben.
- Zu Test- und Entwicklungszwecken kommen ausschließlich Testdaten zum Einsatz.
- Testdaten, die auf Echtdaten basieren, werden anonymisiert.
- Es existiert ein Konzept zur Erstellung und Verwendung von Testdaten.

1. Weitere Informationen zu Zero Trust siehe u.a. https://www.microsoft.com/de-de/security/business/zero-trust und https://www.security-insider.de/was-ist-ein-zero-trust-modell-a-752389/ ↑