ventopay gmbh
Österreich: Hagenberg | Wien
Deutschland: Essen | Augsburg | Hamburg
office@ventopay.com | www.ventopay.com

Technisch-organisatorische Maßnahmen nach Artikel 32 DSGVO

Die nachstehend angeführten technischen und organisatorischen Maßnahmen (TOMs) sind Strategien zur Erfüllung der Anforderungen nach Artikel 32 und Erwägungsgrund 78 der DSGVO und weisen die Einhaltung derer nach.

Vertraulichkeit

Zutrittskontrolle

- Der Schutz vor unbefugtem Zutritt zu den Räumlichkeiten der ventopay erfolgt durch ein elektronisches Schließsystem mittels Token. Die Zutrittsberechtigungen werden über ein Zutrittssystem auf Basis eines rollenbasierten Berechtigungssystems für jeden Raum vergeben.
- Der Token ist erst aktiviert, wenn der Benutzer sich zuvor korrekt angemeldet hat.
- Die Zuordnung des Tokens wird dokumentiert.
- Am Standort Hagenberg werden der Eingangsbereich sowie der Serverraum videoüberwacht. Der Zutritt zum Serverrack im Serverraum ist darüber hinaus mittels mechanischem Schloss abgesichert. Der Schlüssel ist ausschließlich der IT zugänglich.
- Am Standort Augsburg gibt es eine Alarmanlage seitens des Vermieters.
- Der Zutritt unternehmensfremder Personen (Besucher, Wartungspersonal, etc.) wird protokolliert.
- Die Zuordnung von Geräten und Mitarbeiter:innen bzw. Kund:innen erfolgt im Assetmanagementsystem.

Zugangskontrolle

- Die Authentifikation erfolgt mittels (ggf. personalisiertem) Benutzer und Kennwort
- Vor unbefugter Systemnutzung wird mittels Kennwörter und entsprechender Passwortrichtlinien geschützt.
- Zwei-Faktor-Authentifizierung ist für wesentliche interne und externe Systeme sowie Infrastruktur etabliert.
- Automatisierte Sperrmechanismen sind umgesetzt.
- Externer Zugriff erfolgt ausschließlich über VPN.
- Ein Mobile Device Management dient als Endpoint Management System, welches auch Anti-Viren-Software beinhaltet.
- Prozesse zur Ausgabe, Rückgabe und bei Verlust von mobilen Endgeräten sind vorhanden.
- Speichermedien werden verschlüsselt (Notebooks, Smartphones, mobile Datenträger, usw.)

Zugriffskontrolle

- Der Zugriff auf personenbezogene und/oder vertrauliche Informationen wird mittels Berechtigungskonzept auf „Need-To-Know"-Basis und nach dem Least-Privilege-Prinzip erteilt. Zugriff erhalten daher nur jene Personen, die aufgrund ihrer Tätigkeit zu diesem Zugriff befugt sind.
- Die Berechtigungsvergabe erfolgt dokumentiert nach einem Standardprozess auf Basis von Rollen. Administrations- und Benutzerkonten werden getrennt.
- Die vergebenen Berechtigungen werden regelmäßig stichprobenartig überprüft.
- Änderungen oder der Entzug der Benutzerberechtigungen werden dokumentiert.
- Zugriffe werden protokolliert.
- Der Zugriff auf Daten geschieht über kryptografisch gesicherte Wege. Wo dies als notwendig identifiziert wurde, wird auf Host- und Netzwerkebene der Zugriff soweit wie möglich per Firewall eingeschränkt.

- Dokumente werden mittels Aktenvernichter zerstört.
- Datenträger werden physisch gelöscht, bevor sie wiederverwendet werden.
- Es existiert ein dokumentiertes Verfahren zur Vernichtung von Datenträgern.

Trennungskontrolle

- Entwicklungs-, Test- und Produktionssysteme werden getrennt betrieben. Eine logische Mandantentrennung ist aktiv.
- Systeme sind in adäquate Subnetze separiert. Die Kommunikation zwischen Netzsegmenten wird nur für die Kommunikation ermöglicht, die notwendig ist.

Klassifikationsschema für Informationen/Daten

- Es existiert ein Klassifikationsschema für Informationen/Daten und damit einhergehende Verhaltensvorschriften.

Pseudonymisierung

- Es existiert ein Verfahren zur Pseudonymisierung von Endkundendaten.

Geheimhaltung

- Mitarbeiter:innen der ventopay und der zur Leistungserbringung herangezogenen Lieferanten sind auf das Datengeheimnis bzw. zur Vertraulichkeit verpflichtet.
- Sofern nötig und/oder gewünscht, werden Non-Disclosure-Agreements mit Kund:innen abgeschlossen.

Integrität

Weitergabekontrolle

- Das unbefugte Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport wird mittels Verschlüsselung, Virtual Private Networks (VPNs), elektronischer Signatur und/oder Vorgaben für die (persönliche) Weitergabe verhindert.
- Vorgaben zum Umgang mit Cloud-Diensten sind etabliert.
- Das Informationsklassifikationsschema definiert Verhaltensvorschriften zur Weitergabe von Informationen.
- Eine Clean-Desk Policy ist etabliert.

Eingabekontrolle

- Protokollierung von Eingabe, Änderung und Löschung von Daten.
- Die Rechte zur Eingabe, Änderung und Löschung von Daten werden auf Basis des Berechtigungskonzeptes vergeben.

Verfügbarkeit

Verfügbarkeitskontrolle

- Schutz gegen zufällige und mutwillige Zerstörung bzw. Verlust mittels online und offline sowie on-site und off-site Backup- & Recovery Konzept.
- Mehrstufiges Sicherheitskonzept mit Datensicherung in ein Ausweichrechenzentrum.
- Regelmäßige Restore-Tests auf System- und Datenebene werden durchgeführt und dokumentiert.
- Eine unterbrechungsfreie Stromversorgung (USV), Klimatisierungssysteme für Serverräume, Brandfrüherkennungssysteme sowie Redundanzkonzepte sind etabliert.
- Wartungsintervalle werden eingehalten und deren Einhaltung über Wartungsprotokolle dokumentiert.
- Security Checks auf Infrastruktur- und Applikationsebene

- Virenschutzsysteme, Firewallsysteme
- Standardprozesse der IT-Betriebsführung (Change Management, Patchmanagement, usw.)
- Standardprozesse bei Eintritt, Wechsel und Ausscheiden von Mitarbeiter:innen.

Notfallmanagement

- Standardprozesse für den Umgang mit IT-Notfällen sowie Wiederanlaufpläne (Meldewege und Notfallpläne)
- IT-Planung auf Basis von Risikoanalysen bzw. RTO und RPO
- Regelmäßige Notfallübungen sowie Schulungen für Mitarbeiter:innen

Löschfristen

- Es existiert ein definierter und dokumentierter Prozess zum Löschen von Daten bei Erreichen der gesetzlichen bzw. vertraglich bestimmten Löschzeitpunkte

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Organisationskontrolle

- Die ventopay pflegt ein Informationssicherheitsmanagementsystem nach ISO 27001, welches jährlich durch eine externe Stelle überprüft wird.
- Prozesse sowie technische und organisatorische Maßnahmen werden regelmäßig auf Aktualität und Angemessenheit evaluiert und die Ergebnisse dokumentiert.
- Die Rolle des Datenschutzbeauftragten ist nach gesetzlichen Vorgaben bestellt.
- Die Rolle des Information Security Managers ist definiert und zugewiesen.
- Jährliche Schulungen zu aktuellen Themen des Datenschutzes und der Informationssicherheit werden lt. Schulungskonzept für Mitarbeiter:innen durchgeführt und dokumentiert.
- Ein Verfahren zum Vorgehen im Falle einer Datenschutzverletzung ist etabliert.
- Mitarbeiter:innen sind vertraglich zur Einhaltung von Vorgaben zu Datenschutz und Informationssicherheit verpflichtet.

Auftragskontrolle

- Notwendige Vereinbarungen und Verträge werden schriftlich mit Lieferanten abgeschlossen.
- Die Weitergabe von personenbezogenen Daten zur Verarbeitung an externe Dienstleister erfolgt ausschließlich auf Basis von Auftragsdatenverarbeitungsverträgen.
- Standardprozesse zur Lieferantenauswahl und -überprüfung sind etabliert und deren Ergebnisse dokumentiert.

Version/Datum	Änderungen	Freigegeben von
0.1	Ersterstellung	Benedikt Kiesenhofer
1.0/24.5.2018	Freigabe	Johannes Reichenberger
1.0	Review	Benedikt Kiesenhofer Christian Ecker
1.0/4.6.2021	Freigabe	Johannes Reichenberger
1.1	Überarbeitung	Bettina Wächter Benedikt Kiesenhofer
2.0/20.09.2023	Freigabe	Johannes Reichenberger