Anlage - Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

§ 1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Die Büroräume von fino stellen keinen Produktionsstandort im eigentlichen Sinn dar. Die produktive Anwendung läuft ausschließlich in ISO-27001 zertifizierten Rechenzentren.

(a) Fino Büroräume

Die Räumlichkeiten von fino sind durch nachfolgende Maßnahmen ausreichend gegen unbefugten Zutritt abgesichert:

- Ausschließlich gewerblich genutztes Gebäude;
- Wachschutz: Bestreifung der Gebäudeumgebung, anlassbezogene Bestreifung innerhalb des Gebäudes.
- Sämtliche Zugänge sind durch folgende Maßnahmen gegen unbefugten Zutritt abgesichert:
  - Türen grundsätzlich verschlossen;
  - Sicherheitsschlösser;
  - Schlüssel personenbezogen registriert;
  - Dokumentierte Schlüsselausgabe;
  - Personalisiertes Schließsystem auf Transponderbasis;
    - Die Aufzeichnung der Zutritte wird im Bedarfsfall aus der Schließanlage ausgelesen
  - Besucher können sich nur in Begleitung von Mitarbeitern bewegen;

(b) Rechenzentrum

Die Rechenzentren sind durch nachfolgende Maßnahmen ausreichend gegen unbefugten Zutritt abgesichert:

- Zutritt zum Rechenzentrum nur für autorisierten Personen nach Voranmeldung
- Zutrittssicherung durch ein materielles (RFID-Chip) und ein geistiges (PIN) Identifikationsmerkmal: Es wird zwischen fest zugewiesenen und beim Sicherheitsdienst zur Abholung hinterlegten Zutrittsberechtigungen unterschieden. Bei Zutrittsberechtigungen, die zur Abholung hinterlegt sind, wird die Autorisierung durch Kontrolle des Personalausweises sichergestellt. Die Daten werden bei einem Sicherheitsdienst hinterlegt (Whitelist), so wird gewährleistet, dass nur berechtigte Personen das Rechenzentrum betreten können;
- Zutritt zu den einzelnen Kundenschränken oder -flächen ist ausschließlich durch den Kunden und durch das zuständige Personal möglich;
- die Zutrittskontrollsysteme sowie die Alarmanlagen über USV und Netzersatzanlage sind gegen Stromausfall gesichert;

- Videoüberwachung
- Perimeterschutz
- Wachdienst: das Rechenzentrum wird regelmäßig innerhalb vorgegebener Zeitfenster durch einen Wachdienst begangen. Die zu überprüfenden Punkte, welche der Wachdienst in den Rechenzentren zu kontrollieren hat, sind festgelegt. Auffälligkeiten werden berichtet. Die vorgegebenen Laufwege des Wachdienstpersonals werden protokolliert.

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

(a) Es erfolgt eine authentifizierte Benutzeridentifikation, insbesondere dadurch, dass:

- alle technischen Systeme (zentral und dezentral), Hardware und Software Firewall-geschützt sind
- der Zugang zu Servern nur einer begrenzten Anzahl von Personen gestattet wird.
- Mitarbeiter können nur über ihren persönlichen SSH Schlüssel auf Server zugreifen. Diese Mitarbeiter SSH Schlüssel müssen auf jedem Server explizit freigeschaltet werden; beim Austritt eines Mitarbeiters aus der Firma werden alle Zugänge deaktiviert.
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern, keine unpersönlichen Sammelkonten (z.B. „Mitarbeiter-1“)
- Temporäre Bruteforce-Prevention nach fehlgeschlagenen Anmeldeversuchen
- mobile Datenträger (Laptops und Smartphones) gesondert verschlüsselt sind
- Die Nutzung mobiler Endgeräte ist durch Mitarbeitervereinbarungen geregelt.
- jeder Arbeitsrechner ist passwortgeschützt. Passwort-Regelungen sind in einer Passwort-Richtlinie festgehalten.
- Jeder Arbeitsrechner wird bei Verlassen des Arbeitsplatzes gesperrt; automatische passwortgestützte Bildschirm- und Rechnersperre nach 15 Minuten Inaktivität
- Berechtigungen für externe Mitarbeiter sind temporär und beschränkt auf Entwicklerplattformen;
- Externe Mitarbeiter und Besucher nutzen das Gäste WLAN

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

(a) Die unerlaubte Tätigkeit in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen wird im Besonderen verhindert, dadurch, dass:

- die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren;

- jeder Zugriff auf Anwendungen (Eingabe, Veränderung und Löschung) protokolliert wird und ausgewertet werden kann (mindestens für ein Jahr);
- Schutz gegen unberechtigte interne und externe Zugriffe durch Verschlüsselung und Firewalls bestehen.
- Trennung von Entwicklungs-, Test- und Produktivbetrieb auf der Ebene des Hypervisors und Kommunikation der virtuellen Maschinen über einen VPN Tunnel, wobei kein Zugriff der Systeme untereinander möglich ist

1.4. Trennungsgebot

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

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

(a) Die Verarbeitung personenbezogener Daten unter Beachtung der Vorgaben der Pseudonymisierung gemäß Art. 32 Abs. 1 a DSGVO wird insbesondere durch folgende Maßnahmen sichergestellt:

- Internes Regelwerk zu Pseudonymisierung
- Verpflichtung der Mitarbeiter
- Technisch automatisierte Umsetzung des Regelwerks
- Code-Änderungen am Pseudonymisierungsprozess können nur nach gesonderter Freigabe gemerged werden
- Kontrolle durch unangekündigte Stichproben

§ 2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

(a) Die Aspekte der Weitergabekontrolle personenbezogener Daten wird hierdurch umgesetzt, dass:

- Datenkommunikation verschlüsselt gemäß TLS und dem Einsatz von VPN-Technologie eingesetzt wird;

- Serverseitig ein ständig aktualisiertes Firewall und Virenschutzkonzept besteht, Endgeräte werden marktüblich gesichert.
- Email-Nachrichten werden grundsätzlich verschlüsselt versendet. Sonstige Informationen werden – wo möglich – nicht personenbezogen und entsprechend vor der Weitergabe anonymisiert.;
- Eine Speicherung von personenbezogenen Daten auf Datenträgern außerhalb des Rechenzentrums ist nicht vorgesehen. Ein physischer Transport von Datenträgern mit personenbezogenen Daten findet nicht statt.

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

(a) Produkte ohne Datenspeicherung

fino verarbeitet die Daten des Endkunden ohne diese persistent zu speichern. Während der Bearbeitung durch den Endkunden sind die Daten nur auf seinem Eingabegerät verfügbar. Mitarbeiter haben zu keinem Zeitpunkt Zugriff auf persönlichen Daten und können solche entsprechend nicht ändern. Mit Abschluss bzw. Beauftragung des Vorgangs werden die erforderlichen Daten temporär in eine Warteschlange für eine etwaige automatisierte Weiterverarbeitung beziehungsweise Brief-/Fax-/Mailversand gehalten. Nach Zweckerreichung, beispielsweise erfolgreicher Bearbeitung und Versand aller Dokumente, werden sämtliche Dokumente und die Auftragsdaten im automatisierten Verfahren gelöscht.

(b) Produkte mit Datenspeicherung

Bei Produkten, die eine Speicherung der Daten benötigen, ist jede Eingabe, Änderung und Löschung durch die Applikation eindeutig einem User-Login zugeordnet. Eine Protokollierung von allen administrativen Zugriffen schreibender Art auf Datenbankebene ist aktiv, wobei hier der Zeitstempel sowie die Aktion protokolliert wird.
Die Protokolldaten der jeweiligen Anwendungen werden in einem zentralen Logging System gespeichert (Sematext).

§ 3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und rasch wiederhergestellt werden können.

Die Datenhaltung innerhalb einer Cloud-Architektur ist mehrfach redundant gesichert und von der Sache selbst ausfallsicher. Es werden tägliche Backups als Festplattensnapshot in mehrfacher Spiegelung erstellt, die jederzeit als Ersatz für ein laufendes System zurückgespielt werden können. Die Systeme werden fortlaufend überwacht, und bei entsprechenden Lastspitzen Maßnahmen zur Lastverteilung durchgeführt. Sofern ein Server ausfällt, wird dieser mit Hilfe von self-healing neu gestartet.

§ 4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Datenschutzfreundliche Voreinstellungen:
  - Die Werkseinstellungen der Anwendungen sind so gewählt, dasslediglich die zur Erfüllung des Anwendungszwecks erforderlichen Daten erhoben werden.
  - Freiwillige Zusatzangaben durch den Nutzer sind entsprechend gekennzeichnet.
- Datenschutzmanagementsystem:
  - Gesamtheit der konzernweiten Maßnahmen zum Schutz personenbezogener Daten
  - Datenschutzorganisation und Verantwortlichkeiten, Einbindung des Datenschutzbeauftragten, Verzeichnis von Verarbeitungstätigkeiten, Löschkonzept, Datenschutz-Folgeabschätzung, Vertragsmanagement, Verpflichtung der Mitarbeiter, Datenschutz-Schulung, Prozess für die Wahrnehmung von Betroffenenrechten, Prozess für die Meldung von Datenschutzverstößen
- Incident Response Management:
  - Prozess zur Erfassung, Kategorisierung, Priorisierung und Lösung von erkannten bzw. vermuteten Störungen und Sicherheitsvorfällen
  - Schnellstmögliche Wiederherstellung des Service
  - Information der betroffenen Stakeholder
- Definition von Kompetenzen und Kontrollmaßnahmen in Abstimmung mit dem Auftraggeber und Einbindung derselbigen in die Betriebsabläufe
- Verpflichtung der Mitarbeiter auf die Befolgung der DSGVO, das Telekommunikationsgeheimnis (§ 3 TTDSG), das Berufsträgergeheimnis (§ 203 StGB) und das Bankgeheimnis.
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Schriftliche Weisungen zwischen Auftragnehmer und Auftraggeber durch Auftragsverarbeitungsvertrag i.S.d. Art. 28 DSGVO
- Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

Version: 01.09.2022