# Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

der Organisation

fincrm GmbH für das Produkt fincrm

Stand: 01.Juli.2021

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die og. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

## 1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

### 1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Die Mitarbeiter von fincrm GmbH haben keinen Zutritt zu Datenverarbeitungsanlagen o.ä.. Es liegen keine Daten auf dem Rechner. Außerdem sind alle Laptops passwortgeschützt.

Gebäude allgemein von fincrm GmbH:

- Besucher müssen sich bei ihrer Ankunft an- und bei ihrer Abreise abmelden. Während ihres Aufenthalts werden sie von Mitarbeitern begleitet.

Rechenzentrumsräume:

- fincrm Kundendaten werden in Rechenzentren von Domainfactory, Hetzner, (Domainfactory) Netcologne verarbeitet und gespeichert
- Technische organisatorische Maßnahmen bei Hetzner , Domainfactory, Netcologne sind in Anlage 3 zu diesem Vertrag aufgeführt.

## 1.2. Zugangskontrolle

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

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

- Der Benutzer- und Administratorzugriff auf das jeweilige fincrm System beruht auf einem rollenbasierten Zugriffsberechtigungsmodell. Jeder Nutzer erhält eine eindeutige ID, um sicherzustellen, dass alle Systemkomponenten nur von berechtigten Benutzern und Administratoren genutzt werden können.
- Es existieren technische Policies zur Passwortkomplexität und Passwort--Rotation bei der fincrm GmbH
- Passwörter werden immer automatisch generiert
- Bei fincrm gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine vertraglichen Tätigkeiten

durchzuführen. Benutzerkonten werden immer zunächst mit den wenigsten Zugriffsrechten ausgestattet. Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus, muss der entsprechende finCRM Admin die Berechtigungen selber konfigurieren.

- Auf fincrm IT Equipment (z.B. Notebooks) sind Virenscanner installiert, die eine Malware Erkennung und einen E-Mail Filter enthalten.
- Der Zugriff auf fincrm Serversysteme erfolgt SSH-Verschlüsselt („Public key“)
- Alle fincrm Serversysteme speichern Daten ausschließlich auf verschlüsselten Datenträgern ab.
- Die fincrm Serversysteme und die dort verarbeiteten Daten sind auf zwei verschiedene, rechtlich unabhängige Rechenzentrumsbetreiber (Domainfactory, Netcologne) gespiegelt.

## 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. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

- Zugriffsberechtigung auf fincrm Produktivsysteme ist auf einen kleinen Kreis von Mitarbeitern (“fincrm Systemadministratoren”) beschränkt.
- Es existieren keine mobilen Datenträger wie USB-Sticks
- Es gibt intern bestimmte Passwort-Vorgaben für Zugriffe auf auftragsdatenbezogene Zugriffe:
    - 10 Zeichen oder mehr
    - Sonderzeichen + Ziffern + Groß/-Kleinschreibung

- Gültigkeitsdauer 180 Tage

- Es existiert ein internes Kontrollsystem, das sicherstellt, dass die Rechtmäßigkeit für Zugriffe auf lexoffice Produktivsysteme regelmäßig stichprobenartig überprüft und diese Stichprobenkontrollen ebenfalls protokolliert werden

### 1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

- Datensätze unterschiedlicher fincrm Kunden werden in unterschiedlichen Datenbanken und Ordnerstrukturen gesichert.
- Test- und Produktivdaten sind strikt getrennt in unabhängigen Systemen, Entwicklungssysteme sind ebenfalls unabhängig von Test-- und Produktivsystemen
- Unterschiedliche Domains und SSL Zertifikate für Test- und Produktivsysteme

## 2. Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

### 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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

- Datenübertragung zwischen fincrm Serversystemen erfolgt ausschließlich innerhalb eines SSH-Tunnels
- Soweit dies möglich ist, werden Daten zudem nur in anonymisierter oder pseudonymisierter Form weitergeben (Passwortgesicherte Zip.Dateien oder Email-Verschlüsselung)
- Bereitstellung über verschlüsselte Verbindungen wie sftp, https

### 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. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten auf den Serversystemen
- In der Anwendung fincrm kann nachvollzogen werden, wer, wann welche Daten geändert hat. Dies wird in der Datenbank protokolliert.

## 3. Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 lit. b DSGVO

### 3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

- Es werden regelmäßig automatische Sicherungskopien und Backups aller fincrm Daten erstellt
- Es gibt ein dediziertes Konzept zur Rekonstruktion der Datenbestände und zudem eine regelmäßige Überprüfung, dass die Datensicherungen auch tatsächlich wieder eingespielt werden können (Datenintegrität der Backups)
- Es existiert ein Notfallkonzept für fincrm mit namentlich benannten Verantwortlichen
- Das Notfallkonzept wird regelmäßig überprüft und aktualisiert
- Mitarbeiter werden in regelmäßigen Abständen auf dieses Notfallkonzept geschult.
- Backups und Sicherungskopien sind über mehrere redundante Serversysteme und Rechenzentrumsstandorte verteilt
- finCRM Produktivsysteme sind mehrfach redundant ausgelegt
- Zur Ausstattung der Rechenzentren von Domainfactory, , NanoComp vgl. Technisch organisatorische Maßnahmen bei Domainfactory in Anlage 3 zu diesem Vertrag

### 3.2. Rasche Wiederherstellbarkeit gem. Art 32 Abs. 1 lit. c DS-GVO

- Mehrfach- redundante Auslegung von Serversystemen und Datenbanken
- Backups werden regelmäßig auf Wiedereinspielbarkeit geprüft
- Es gibt regelmäßige Notfallübungen, in denen Teams u.a. Wiederherstellungsszenarien üben (LINK)

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO

### 4.1. Datenschutz-Management

- Regelmäßige Sensibilisierung der Mitarbeiter über den Datenschutz
- Schulung der Angestellten und auf Vertraulichkeit/Datengeheimnis verpflichtet
- Die Organisation kommt den Informationspflichten nach Art. 14 und 14 DSGVO nach. (Auf Anfrage der Benutzer)
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

## 4.2. Incident-Response-Management

- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/ Datenpannen
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Ticketsystem zur Erfassung von Sicherheitsvorfällen o.ä.
- Technische Maßnahmen werden vom Serverprovider durchgeführt - Anlage 3

## 4.3. Datenschutzfreundliche Voreinstellung (Art. 25 Abs. 2 DSGVO)

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

## 4.4. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

- Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Verantwortlichen
- Klare, eindeutige Weisungen
- Verhinderung von Zugriffen unbefugter Dritter auf die Daten
- Verbot, Daten in unzulässiger Weise zu kopieren
- Vereinbarungen über Art des Datentransfers und deren Dokumentation
- Kontrollrechte durch den Auftraggeber
- Vereinbarung von Vertragsstrafen
- strenge Auswahl der Dienstleister
- Nachkontrollen