

**Richtlinie der
TREND Wirtschaftstreuhandgesellschaft m.b.H.**

Paracelsusstraße 13
5020 Salzburg

zur Gewährleistung der Sicherheit personenbezogener Daten

Zur Gewährleistung der Sicherheit personenbezogener und sensibler Daten (in Folge nur personenbezogene Daten) werden von der Kanzlei folgende Sicherheitsmaßnahmen in Entsprechung des Art 32 der Datenschutz-Grundverordnung (DSGVO) implementiert:

I. Präventive Sicherheitsmaßnahmen – Maßnahmen zur Verhinderung eines erfolgreichen Angriffs

- Technische Maßnahmen
 - **Logische Zugriffskontrolle:** Die Vergabe von Zugriffsberechtigungen erfolgt ausschließlich nach dem Bemessen vom Geschäftsführer. Ein entsprechendes „Need-to-Know“-Prinzip wird der Vergabe von Zugriffsberechtigungen zugrunde gelegt.
 - **Authentifizierung:** Jeglicher Zugriff auf personenbezogene Daten erfolgt ausschließlich nach einer erfolgreichen Authentifizierung.
 - **Passwortsicherheit:** Für die Passwörter zur Authentifizierung gelten folgende Vorgaben:
 - 8 bis 16 stellig
 - Mindestens ein Groß- und ein Kleinbuchstabe
 - Mindestens eine Zahl oder Sonderzeichen
 - **Verschlüsselung auf dem Übertragungsweg:** Personenbezogene Daten werden ausschließlich über verschlüsselte E-Mails, per Post oder per Fax - zumindest soweit es sich um Daten der Lohnverrechnung oder sensible Daten handelt - übermittelt.
 - **Verschlüsselung mobiler Geräte:** Soweit mobile Endgeräte und mobile Datenträger im Einsatz sind, werden diese verschlüsselt, zumindest soweit auf diesen Geräten Daten der Lohnverrechnung oder sensible Daten gespeichert werden.
 - **Netzwerksicherheit:** Es wird eine Firewall und ein aktiver Viren- und Webfilter eingesetzt, welche das interne Netzwerk vom Internet trennt und – soweit notwendig – eingehenden Netzwerkverkehr blockiert.
 - **Maßnahmen gegen Schadsoftware:** Auf allen Systemen ist eine Anti-Viren Software (Kaspersky Internet Security– Vollversion) eingesetzt. Alle eingehenden E-Mails und Dateien werden automatisch auf Schadsoftware gescannt.
 - **Management von Sicherheitslücken:** Soweit möglich, wird auf allen Geräten die automatische Installation von Sicherheitsupdates aktiviert. Ansonsten erfolgt die Installation kritischer Sicherheitsupdates binnen 3 Arbeitstagen, die Installation von Sicherheitsupdates mittlerer Kritikalität binnen 25 Arbeitstagen und die Installation von Sicherheitsupdates geringer Kritikalität binnen 40 Arbeitstagen.

– Organisatorische Maßnahmen

- **Klare Zuständigkeiten:** Interne Zuständigkeiten für Fragen der Datensicherheit werden definiert.
- **Verschwiegenheitspflicht der Dienstnehmer:** Die Dienstnehmer werden über die Dauer ihres Dienstverhältnisses hinaus zur Verschwiegenheit verpflichtet. Insbesondere werden sie dazu verpflichtet, personenbezogene Daten nur auf ausdrückliche Anweisung des Vorgesetzten an Dritte zu übermitteln.
- **Schulungen und Informationsmaßnahmen:** Die Dienstnehmer werden zu Fragen der Datensicherheit (intern oder extern) geschult und angemessen über Fragen der Datensicherheit informiert (z.B. Passwortsicherheit).
- **Geordnete Beendigung des Dienstverhältnisses:** Bei Beendigung des Dienstverhältnisses erfolgt eine unverzügliche Sperrung aller Konten des ausscheidenden Dienstnehmers sowie eine Abnahme aller Schlüssel des ausscheidenden Dienstnehmers.
- **Verwaltung von Computer-Hardware:** Es werden Aufzeichnungen darüber geführt, welchem Mitarbeiter welche Endgeräte (z.B. PC, Laptop, Mobiltelefon) zugewiesen wurden.
- **Eingabekontrolle:** Es bestehen Verfahren zur Kontrolle der Richtigkeit der eingegebenen personenbezogenen Daten.
- **Keine Doppelverwendung von Benutzer-Accounts:** Jede Person hat ihren eigenen Benutzer-Account – das Teilen von Benutzer-Accounts ist nicht möglich.
- **Keine unnötige Verwendung administrativer Accounts:** Benutzer-Accounts mit administrativen Rechten werden nur in Ausnahmefällen verwendet – die reguläre Nutzung von IT-Systemen erfolgt ohne administrative Rechte.
- **Auswahl der Dienstleister:** Bei der Auswahl von Dienstleistern wird das vom Dienstleister gebotene Datensicherheitsniveau berücksichtigt. Der Einsatz eines Dienstleisters, der als Auftragsverarbeiter einzustufen ist, erfolgt nur nach Abschluss einer Auftragsverarbeitervereinbarung.
- **Sichere Datenentsorgung:** Papier, welches personenbezogene Daten enthält, wird einem externen Dienstleister zur sicheren Vernichtung übergeben. Datenträger werden vor ihrer Entsorgung vollständig überschrieben oder physisch zerstört, sodass die darauf gespeicherten Daten nicht wieder hergestellt werden können.

– Physische Maßnahmen

- **physische Zugangskontrolle:** Das Betreten der Betriebsräumlichkeiten ist für betriebsfremde Personen nur in Begleitung einer betriebsangehörigen Person zulässig und möglich.
- **Einbruchssicherheit:** Die Zugänge zu den Betriebsräumlichkeiten verfügen über einen angemessenen Einbruchsschutz (Sicherheitstüren, vergitterte Fenster im Erdgeschoss, Hinweis auf Alarmanlage).
- **Schlüsselverwaltung:** Schlüssel, welchen den Zugang zu den Betriebsräumlichkeiten oder Teilen derselben ermöglichen, werden nur an besonders vertrauenswürdige Personen ausgehändigt und dies auch nur soweit und solange diese Personen tatsächlich einen eigenen Schlüssel benötigen.

II. Detektive Sicherheitsmaßnahmen – Maßnahmen zur Erkennung eines Angriffs

- Technische Maßnahmen
 - **Scans nach Schadsoftware:** Es werden regelmäßig Scans nach Schadsoftware (Anti-Viren-Scans) durchgeführt, um Schadsoftware zu identifizieren, welche ein IT-System bereits kompromittiert hat.
 - **Sicherheits-Mailing-Listen:** Es wird sichergestellt, dass ein Mitarbeiter des Unternehmens oder ein externer Dienstleister einschlägige Mailing-Listen für die Bekanntgabe neuer IT-Sicherheits-Bedrohungen abonniert (z.B. Mailing-Listen der Hersteller der verwendeten Software), um über die aktuelle Bedrohungslage in Kenntnis zu sein.
- Organisatorische Maßnahmen
 - **Erkennung von Sicherheitsverletzungen durch Dienstnehmer:** Alle Dienstnehmer werden instruiert, wie sie Sicherheitsverletzung erkennen können (z.B. nicht mehr auffindbare Computer-Hardware, Meldungen von Anti-Viren-Software).
 - **Betriebsfremde Personen:** Alle Dienstnehmer werden instruiert, betriebsfremde Personen anzusprechen, sollten sie in den Betriebsräumlichkeiten angetroffen werden.
 - **Audits:** Es werden regelmäßige Audits durchgeführt (z.B. Prüfung, ob alle kritischen Sicherheits-Updates installiert wurden). Insbesondere erfolgt eine Prüfung der erteilten Zugriffs- und Zutrittsberechtigungen (welchem Mitarbeiter ist welcher Benutzer-Account mit welchen Zugriffsrechten zugewiesen; welche Personen verfügen über welche Schlüssel).

III. Reaktive Sicherheitsmaßnahmen – Maßnahmen zur Reaktion auf einen Angriff

- Technische Maßnahmen
 - **Datensicherung:** Es werden regelmäßig Datensicherungen erstellt und sicher aufbewahrt.
 - **Datenwiederherstellungskonzept:** Es wurde ein Konzept zur raschen Wiederherstellung von Datensicherungen entwickelt, um nach einer Sicherheitsverletzung zeitnah den regulären Betrieb wieder herstellen zu können.
 - **Automatische Entfernung von Schadsoftware:** Die eingesetzte Anti-Viren-Software verfügt über die Funktion, Schadsoftware automatisch zu entfernen.
- Organisatorische Maßnahmen
 - **Meldepflicht für Dienstnehmer:** Alle Dienstnehmer werden angewiesen, Sicherheitsverletzungen unverzüglich an eine zuvor definierte interne Stelle bzw. Person zu melden.
 - **Meldepflicht für externe Dienstleister:** Allen Dienstleistern wurden Kontaktdaten für die Meldung von Sicherheitsverletzungen mitgeteilt.
 - **Prozess für die Reaktion auf Sicherheitsverletzungen:** Es wird durch einen geeigneten Prozess sichergestellt, dass Sicherheitsverletzungen innerhalb von 72

Stunden ab Kenntnis von der Sicherheitsverletzung an die Datenschutzbehörde gemeldet werden können. Insbesondere sind allen Dienstnehmern die Notfall-Telefonnummern der zu involvierenden Personen bekannt zu geben (z.B. Notfall-Telefonnummer für den IT-Support).

- Physische Maßnahmen
 - **Feuerlöscher:** In den Betriebsräumlichkeiten gibt es eine geeignete Anzahl an Feuerlöschern. Allen Dienstnehmern ist bekannt, wo sich die Feuerlöscher befinden.
 - **Feueralarm:** Soweit es keinen Brandmelder gibt, der über keine automatische Verbindung zur Feuerwehr verfügt, wird durch einen angemessenen Prozess sichergestellt, dass die Feuerwehr manuell verständigt werden kann.

IV. Abschreckende Sicherheitsmaßnahmen – Maßnahmen zur Minderung der Angreifermotivation

- Technische Maßnahmen
 - **Automatische Warnmeldungen:** Nutzer erhalten automatische Warnmeldungen bei risikoträchtiger IT-Nutzung (z.B. durch den Webbrowser, wenn eine verschlüsselte Website kein korrektes SSL/TLS-Zertifikat verwendet).
- Organisatorische Maßnahmen
 - **Sanktionen bei Angriffen durch eigene Dienstnehmer:** Alle Dienstnehmer werden darüber informiert, dass Angriffe auf betriebseigene IT-Systeme nicht toleriert werden und schwerwiegende arbeitsrechtliche Konsequenzen, wie insbesondere eine Entlassung nach sich ziehen können.