

RICHTLINIE der
OVILAVA Wirtschaftsprüfungs- und Steuerberatungsges.m.b.H
zur Gewährleistung der Sicherheit personenbezogener Daten

Zur Gewährleistung der Sicherheit personenbezogener Daten werden von der Kanzlei folgende Sicherheitsmaßnahmen in Entsprechung des Artikel 32 der Datenschutz-Grundverordnung implementiert:

Präventive Sicherheitsmaßnahmen – Maßnahmen zur Verhinderung eines erfolgreichen Angriffs

Technische Maßnahmen:

- **Logische Zugriffskontrolle:** Die Vergabe von Zugriffsberechtigungen erfolgt nach dem „Need-to-Know“-Prinzip.
- **Authentifizierung:** Jeglicher Zugriff auf personenbezogene Daten erfolgt ausschließlich nach einer erfolgreichen Authentifizierung.
- **Passwortsicherheit:** Soweit Passwörter zur Authentifizierung eingesetzt werden, sollten diese mindestens 8 Zeichen lang sein und aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen bestehen. Passwörter werden ausschließlich verschlüsselt gespeichert.
- **Verschlüsselung auf dem Übertragungsweg:** Personenbezogener Daten werden auf dem Übertragungsweg über das Internet verschlüsselt, zumindest soweit es sich um Daten der Lohnverrechnung oder sensible Daten handelt.
- **Netzwerksicherheit:** Es wird eine Firewall eingesetzt, welche das interne Netzwerk vom Internet trennt und – soweit möglich – eingehenden Netzwerkverkehr blockiert.
- **Maßnahmen gegen Schadsoftware:** Es wird nach Möglichkeit auf allen Systemen Anti-Viren Software eingesetzt. Alle eingehenden E-Mails 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.
- **Bildschirm Sperre:** Bei sämtliche Geräten ist eingestellt, dass eine Bildschirmsperre nach spätestens 10 Minuten Nichtbenutzung des Computers diesen automatisch sperrt, sodass dieser erst wieder nach Eingabe eines Kennworts verwendet werden kann. Es ist somit sichergestellt, dass beim Verlassen des Arbeitsplatzes der Computer so gesperrt ist, dass er durch Dritte nicht genutzt werden kann (Stichwort: Bildschirmsperre).
- **Umgang mit Speichermedien:** Sämtliche Computer sind so gesperrt sind, dass Speichermedien nur nach Eingabe eines Passworts verwendet werden können.
- **Sichere Nutzung des Internets:** Der Verantwortliche stellt sicher, dass Benutzer eine Schulung zum sicheren Umgang mit dem Internet erhalten. Die Schulung der Mitarbeiter erfolgt einmal im Jahr.
- **Technische Maßnahmen zum Sichern von Arbeitsplatzrechnern:** Der Verantwortliche stellt sicher, dass sämtliche Arbeitsplatzrechner so gesichert sind, dass Rechnermikrofone und Kameras gegen unberechtigten Zugriff gesperrt sind. Sämtliche Arbeitsplatzrechner erhalten regelmäßig Sicherheitsupdates und werden regelmäßig auf Viren untersucht. Die Grundkonfiguration der Rechner

sieht vor, dass die Rechner vor unberechtigtem Zugang geschützt sind (die Nutzung des Rechners ist nur nach Eingabe eines Passworts möglich).

- **Datensicherung der Clients:** Der Verantwortliche stellt sicher, dass sämtliche lokal auf den Arbeitsplatzrechnern gespeicherten Daten regelmäßig gesichert werden

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 eines 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 sollte ihren eigenen Benutzer-Account haben – das Teilen von Benutzer-Accounts ist untersagt.
- **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 grundsätzlich geschreddert bzw. 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.
- **Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung:** Der Verantwortliche stellt sicher, dass sämtliche Nutzer sich verpflichten, sich nach dem Erfüllen einer Aufgabe vom jeweiligen Arbeitsplatzrechner abzumelden.
- **Geeigneter Umgang mit Laufwerken für Wechselmedien und externe Datenträger (Handhabung, Entsorgung, Transport):** Den Mitarbeitern ist es ohne explizite Erlaubnis nicht gestattet, personenbezogene Daten, die der Verantwortliche verarbeitet, auf Datenträger zu speichern. Eine solche Speicherung wird der jeweilige Verantwortliche explizit anordnen und – für den Einzelfall – geeignete Sicherheitsmaßnahmen anordnen.

Physische Maßnahmen

- **physische Zugangskontrolle:** Das Betreten der Betriebsräumlichkeiten ist für betriebsfremde Personen nur in Begleitung einer betriebsangehörigen Person zulässig.
- **Einbruchssicherheit:** Die Zugänge zu den Betriebsräumlichkeiten verfügen über einen angemessenen Einbruchsschutz (Alarmanlage).
- **Besonderer Schutz von Computer-Hardware:** Der Zugang zu Räumlichkeiten, in denen sich Computer-Server befinden ist durch besondere Maßnahmen gesichert (z.B. zusätzliches Schloss).
- **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.
- **Regeln zum Verlassen der Räumlichkeiten:** Der Verantwortliche stellt sicher, dass die Mitarbeiter dahingehend geschult werden, dass sämtliche Fenster und Türen bei Verlassen der Räumlichkeiten geschlossen bzw. abgeschlossen werden, sodass ein unbefugter Dritter keinen Zugang zu den Räumlichkeiten des Verantwortlichen bzw. zu personenbezogenen Daten hat.
- **Regelungen zu Home-Office, mobiler Arbeitsplatz:** Der Verantwortliche stellt sicher, dass Mitarbeiter, welche einen mobilen Arbeitsplatz oder das Homeoffice nutzen, sich verpflichten sämtliche Zugangsdaten geheim zu halten. Das schriftliche Festhalten der Zugangsdaten ist nicht zulässig. Der Verantwortliche stellt sicher, dass die Mitarbeiter dem Verantwortlichen umgehend mitteilen, sollten die Zugangsdaten des Mitarbeiters nicht mehr geheim sein.
- **Regelungen zu Bring your own device:** Sollte der Verantwortliche den Mitarbeitern gestatten, eigene Endgeräte (Smartphones, Tablets, Laptops) zu nutzen, wird der Verantwortliche eine entsprechende Richtlinie erlassen und den Mitarbeitern zur Kenntnis bringen.
- **Sicherung von physischen Dokumenten:** Der Verantwortliche stellt sicher, dass sämtliche Mitarbeiter dahingehend geschult werden, dass Dokumente der Kategorie „**besonders vertraulich**“ in einem verschlossenen Aktenordner oder Aktenschrank oder in einem verwahrt und unmittelbar nach dem Gebrauch wieder eingeschlossen werden müssen oder in einem absperrbaren Raum befinden. Der Verantwortliche hat mit den Mitarbeitern geeignete Maßnahmen zur Sicherung des Schlüssels getroffen.
- **Arbeitsplatzrechner:** Der Verantwortliche stellt sicher, dass Computer vor unbefugtem Zugriff und unbefugter Nutzung geschützt sind. Darüber hinaus sind sämtliche Arbeitsplatzrechner so konfiguriert, dass sich Updates und Softwarekorrekturen, die Sicherheitslücken schließen, automatisch installieren. Bei Arbeitsplatzrechnern, auf denen besondere Kategorien von Daten gespeichert sind, sind die genutzten Speichermedien verschlüsselt.
- **Mobiltelefone:** Sofern auf mobilen Endgeräten (Mobiltelefone, Tablets oder Ähnliches) personenbezogene Daten gespeichert werden, wird der Verantwortliche Maßnahmen dahingehend ergreifen, dass der Zugriff auf die mobilen Endgeräte erst nach Eingabe eines Kennworts möglich ist. Mobile Endgeräte sind darüber hinaus so konfiguriert, dass sich der Bildschirm des mobilen Endgeräts nach spätestens 30 Sekunden sperrt, sodass das Endgerät erst nach Eingabe eines Kennworts wiederverwendet werden kann.
- **Sicherung von öffentlich zugänglichen Bereichen:** Sofern der Verantwortliche öffentlich zugängliche Netzwerke („WLAN“) betreibt, wird er diese so sichern, dass ein Zugriff auf nicht öffentlich zugängliche Systeme des Verantwortlichen nicht möglich ist. Der Verantwortliche stellt ferner sicher, dass öffentlich zugängliche Netzwerkanschlüsse (etwa Netzwerkdosen) nicht genutzt werden können.

○ **Nutzung von Kommunikationsmitteln:**

Der Verantwortliche klassifiziert Dokumente wie folgt: „besonders vertraulich“/“vertraulich“/“nicht vertraulich“/“öffentlich bekannt“. Der Verantwortliche nutzt folgende Kommunikationsmedien:

- Persönliche Übergabe
- Versand per verschlüsselter elektronischer Kommunikation
- Versand per eingeschriebenem Brief
- Versand per Post
- Versand per Fax
- Versand per E-Mail
- Telefonische Mitteilung

Zur Einhaltung eines angemessenen Sicherheitsniveaus verpflichtet sich der Verantwortliche, Informationen ausschließlich wie folgt zu übermitteln bzw. zu übersenden:

Klassifizierung	Kommunikationsmedium
besonders vertraulich	Versand per Post Persönliche Übergabe
Vertraulich	Persönliche Übergabe Versand per verschlüsselter elektronischer Kommunikation (Übertragungsweg) Versand per Post
Nicht vertraulich	Jedes Medium
Öffentlich bekannt	Jedes Medium

Der Verantwortliche klassifiziert Informationen wie folgt:

Information	Klassifizierung
Stammakteninformation	vertraulich
Adressinformationen	vertraulich
Kontaktinformationen	vertraulich
Kundeninformation	vertraulich
Mitarbeiterstammakten und -informationen	besonders vertraulich

Die Weitergabe von Zugangsdaten und Passwörtern im Zusammenhang mittels verschlüsselter elektronischer Kommunikation erfolgt ausschließlich per Post oder persönlich (nach vorheriger schriftlicher Einwilligungserklärung des Empfängers).

Der Verantwortliche verpflichtet sich, vertrauliche Informationen an zulässige Übermittlungsempfänger ausschließlich mittels verschlüsselter elektronischer Kommunikation oder mittels Fax zu senden. (TLS)

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.
- **Automatische Prüfung von Logfiles:** Soweit die Sicherheits-Logfiles mehrerer System auf einem System zentralisiert gesammelt werden, erfolgt eine automatisierte Auswertung der Logfiles, um mögliche Sicherheitsverletzungen zu erkennen.
- **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 regelmäßige Prüfung der erteilten Zugriffs- und Zutrittsberechtigungen (welchem Mitarbeiter ist welcher Benutzer-Account mit welchen Zugriffsrechten zugewiesen; welche Personen verfügen über welche Schlüssel).
- **Manuelle Prüfung von Logfiles:** Soweit Logfiles geführt werden (z.B. über erfolglose Authentifizierungsversuche), werden diese in regelmäßigen Abständen geprüft.
- **Serverraum:** Der Verantwortliche stellt sicher, dass Server vor unberechtigtem Zugriff geschützt (er ist extra ersperrt und in einem alarmgesicherten Bereich) sind und eine Verfügbarkeit des Servers in ausreichendem Ausmaß sichergestellt ist.
- **Archiv:** Der Verantwortliche hat Maßnahmen dahingehend ergriffen, dass der Zutritt zum Archiv nur berechtigten Personen möglich ist.

Physische Maßnahmen

- **Brandmelder:** Sofern dies aufgrund der Größe und Beschaffenheit der Betriebsräumlichkeiten angemessen ist, wird ein Brandmelder installiert, der durch Rauch automatisch ausgelöst wird.

Reaktive Sicherheitsmaßnahmen – Maßnahmen zur Reaktion auf einen Angriff

Technische Maßnahmen

- **Datensicherung:** Es werden regelmäßig Datensicherungen erstellt und sicher aufbewahrt.
- **Datenwiederherstellungskonzept:** Es wird 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.

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.

Sonstiges

- **Behandlung von Sicherheitsvorfällen:** Der Verantwortliche hat Prozesse definiert, was im Fall eines Sicherheitsvorfalles passieren soll.
- **Überprüfung der Einhaltung:** Der Verantwortliche wird regelmäßig die hier beschriebenen technischen und organisatorischen Maßnahmen evaluieren und prüfen.