UBK
STEUERBERATUNG
UNTERNEHMENSBERATUNG

Sicherheitsrichtlinie der

UBK SteuerberatungsgmbH
UBK UnternehmensberatungsgmbH

zur Gewährleistung 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
  - **Authentifizierung**: Jeglicher Zugriff auf personenbezogene Daten erfolgt ausschließlich nach einer erfolgreichen Authentifizierung.
  - **Passwortsicherheit**: Soweit Passwörter zur Authentifizierung eingesetzt werden, werden diese mindestens 8 Zeichen lang sein und aus Klein- und Großbuchstaben, 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.
  - **Verschlüsselung mobiler Geräte**: Mobile Endgeräte und mobile Datenträger werden verschlüsselt, zumindest soweit auf diesen Geräten Daten der Lohnverrechnung oder sensible Daten gespeichert werden.
  - **Netzwerksicherheit**: Es ist eine Firewall eingesetzt, welche das interne Netzwerk vom Internet trennt und – soweit möglich – eingehenden Netzwerkverkehr blockiert.
  - **Maßnahmen gegen Schadsoftware**: Es ist auf allen Systemen eine Anti-Viren Software eingesetzt. Alle eingehenden E-Mails werden automatisch auf Schadsoftware gescannt.
  - **Management von Sicherheitslücken**: Es ist 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 ist definiert.
    - **Verschwiegenheitspflicht der Dienstnehmer**: Die Dienstnehmer sind über die Dauer ihres Dienstverhältnisses hinaus zur Verschwiegenheit verpflichtet. Insbesondere sind sie dazu verpflichtet, personenbezogene Daten nur auf ausdrückliche Anweisung eines Vorgesetzten an Dritte zu übermitteln.
    - **Schulungen und Informationsmaßnahmen**: Die Dienstnehmer sind zur 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, einschließlich der Codekarte der Alarmanlage 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 ausgeschlossen.
    - **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.

- Physische Maßnahmen
    - **physische Zugangskontrolle**: Das Betreten der Betriebsräumlichkeiten ist für betriebsfremde Personen nur in Begleitung einer betriebszugehörigen Person zulässig.
    - **Einbruchssicherheit**: Die Zugänge zu den Betriebsräumlichkeiten verfügen über einen angemessenen Einbruchsschutz, einer Alarmanlage.
    - **Besonderer Schutz von Computer-Hardware**: Der Zugang zu Räumlichkeiten, in denen sich Computer-Server befinden ist durch besondere Maßnahmen, eines Bewegungsmelders unserer Alarmanlage gesichert.
    - **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.

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.

- 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.

- Physische Maßnahmen
    - **Brandmelder**: Es sind drei Brandmelder an unserer Alarmanlage angeschlossen.

Reaktive Sicherheitsmaßnahmen – Maßnahmen zur Reaktion auf einen Angriff

- Technische Maßnahmen
    - **Datensicherung**: Es werden täglich Datensicherungen in mehreren Generationen erstellt und sicher aufbewahrt (Sicherheitsschrank sowie außerhalb der Geschäftsräumlichkeiten).
    - **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 automatische zu entfernen.

- Organisatorische Maßnahmen
    - **Meldepflicht für Dienstnehmer**: Alle Dienstnehmer sind 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 wurden 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 und Löschdecken. 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 sind darüber informiert, dass Angriffe auf betriebseigene IT-Systeme nicht toleriert werden und schwerwiegende arbeitsrechtliche Konsequenzen, wie insbesondere eine fristlose Entlassung nach sich ziehen.

Unsere Kontaktdaten

Sollten Sie zu dieser Sicherheitsrichtlinie Fragen haben, wenden Sie sich bitte an uns:

UBK SteuerberatungsgmbH
UBK UnternehmensberatungsgmbH
beide in 1070 Wien, Schottenfeldgasse 69/1
office@ubk.at