Steuerberatersozietät
Pirlet & Schröder

Sozietätspartner
Daniel Pirlet
Dipl. Kfm. Steuerberater
Magdalena Schröder
Steuerberaterin
Felix Schröder
Dipl. BetrW (FH), Steuerberater

Kinkelstr. 3
50935 Köln (Lindenthal)
Telefon (0221) 8608 114
Telefax (0221) 8608 123
Internet: www.StB-Pirlet.de
E-Mail: Info@StB-Pirlet.de

Technische und organisatorische Maßnahmen (ToM)
gemäß Art. 32 EU-DSGVO der

Steuerberatersozietät
Pirlet & Schröder

Kinkelstr. 3, 50935 Köln
Tel.: +49 (0)221 / 8608 114
Fax: +49 (0)221 / 8608 113
E-Mail: info@StB-Pirlet.de

Datenschutzbeauftragter

DACO – GmbH
Datencooperation & Unternehmensberatung
Kinkelstr. 3, 50935 Köln
Geschäftsführer: Dorothee Pirlet
Tel.: +49 (0)221 / 8608 114
Fax: +49 (0)221 / 8608 113
E-Mail: DACO-GmbH@StB-Pirlet.de

Vorwort

Für die Steuerberatersozietät Pirlet und Schröder ist es ein besonderes Anliegen die Persönlichkeitsrechte Ihrer Mandanten in Bezug auf Datenschutz und die Datensicherheit jederzeit zu gewährleisten. Wobei wir neben den Vorgaben der Datenschutzverordnung (DSGVO) einer besonderen Verschwiegenheitsverpflichtung gemäß § 203 StGB unterliegen.

Daher hat die Steuerberatersozietät Schutzmaßnahmen für jeglichen Umgang mit vertraulichen oder sicherungsbedürftigen Daten etabliert, die im Rahmen des technischen Fortschritts stetig weiter entwickelt werden.

Als Steuerberatersozietät erfüllen wir in erster Linie einen Steuerberatungsauftrag und sind als Berufsgeheimnisträger gem. § 203 StBG keine Auftragsverarbeiter, für den bei der Verarbeitung (einschließlich Übermittlung) personenbezogener Daten eine Rechtsgrundlage gemäß Art. 6 DS-GVO gegeben sein muss. Dieses gilt auch für die Erstellung der laufenden Lohn- und Gehaltsabrechnungen für unsere Mandanten.

Technische und organisatorische Maßnahmen (ToM)

Nachfolgend befindet sich die Beschreibung der „technischen und organisatorischen Maßnahmen (ToM)" der Steuerberatersozietät Pirlet & Schröder (,,Sozietät") am Standort Kinkelstr. 3,50935 Köln gemäß Art. 32 Abs. 1 EU-DSGVO.

Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen behält sich die Sozietät vor, sofern das Schutzniveau nach EU-DSGVO nicht unterschritten wird.

1. Pseudonymisierung

Grundsätzlich können Daten mit einem Pseudonym, d.h., einem nicht personenbezogenen Namen, einer Nummer oder Ähnlichem versehen werden, welch es eine Zuordnung erschwert. Wichtig für eine wirksame Pseudonymisierung ist dabei, dass die pseudonymisierten Daten ohne Hinzuziehung zusätzlicher Informationen keine Zuordnung erlauben. Im Rahmen der Auftragserfüllung ordnet die Sozietät jedem Mandanten bzw. Kunden eine neutrale Mandantennummer zu, unter der die Daten gespeichert werden. Darüber hinaus trifft die Sozietät keine Maßnahmen zur Pseudonymisierung.

2. Verschlüsselung

Daten können verschlüsselt werden. Hierbei wird die Information mit Hilfe eines kryptografischen Verfahrens in eine nicht leserbare Zeichenfolge verwandelt. Bei der Nutzung der Verschlüsselung bleibt der Personenbezug der Daten erhalt en. Die Daten werden Jedoch auf Basis von mathematischen Algorithmen so verändert, dass sie ohne Kenntnis des zu gehörigen Schlüssels mit der aktuell verfügbaren Technik nicht lesbar gemacht werden können.

Zur Verschlüsselung setzt die Sozietät für den elektronischen Transport Verschlüsselungsverfahren ein, die dem Stand der Technik entsprechen und ein Schutz-niveau erreichen, das den Anforderungen z. B. von Berufsgeheimnisträgern (wie Steuerberatern, Wirtschaftsprüfern, Rechtsanwälten, Ärzten usw.) angemessen ist.

Dies ist für den elektronischen Transport zwischen der Sozietät

- und dem Rechenzentrum der Datev e.G.: über VPN - oder TLS - Verbindung mit Zertifikaten oder Zwei -Faktor Authentifikation abgesichert.
- und dem Rechenzentrum der Finanzverwaltung und sonstigen Behörden: über VPN - oder TLS - Verbindung mit Zertifikaten oder Zwei -Faktor Authentifikation abgesichert.
- und Einzelpersonen: abgesichert mit Verschlüsselungsverfahren nach dem Stand der Technik
- Mobile Endgeräte der Sozietätsmitarbeiter (Smartphones, Tablets, Notebooks) werden - sofern hier personenbezogene Daten verarbeitet werden - verschlüsselt und mit Passwort, Fingerabdruck oder Pin geschützt.

3. Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste

Maßnahmen sollen die Vertraulichkeit der verwendeten Systeme & Dienste schützen. Es soll verhindert werden, dass es zu unbefugter oder unrechtsmäßiger Verarbeitung kommt. Hierunter fallen Maßnahmen, welche den Zutritt, Zugang und Zugriff auf Systeme und Dienstregeln (Beispiele: Räumliche Maßnahmen, Zugangskontrollen. Zugriffsrechte, Alarmanlagen). Ebenso soll die Integrität der Systeme geschützt werden. Daten sollen stets richtig und verlässlich sein und dürfen nicht unbeabsichtigt oder schadhaft geändert oder zerstört werden können.

3.1. Vertraulichkeit

Unbefugten ist der Zutritt zu den Datenverarbeitung-, Datenspeicherung-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten), mit denen Daten im Auftrag verarbeitet werden, zu verwehren. Die Vertraulichkeit von Systemen (Hardware) und Diensten (Software) setzt im Rahmen der Verarbeitung zwingend ein Zugriffskonzept voraus, das mit Gruppen - und Benutzer rechten arbeitet und den Zugriff auf einzelne Daten im Rahmen der Verarbeitung, erforderlichen Prozessen ermöglicht. Hierzu gehören auch Maßnahmen der Zutrittskontrolle, der Zugangskontrolle und der Zugriffkontrolle.

Alle im Auftrag verarbeiteten Daten des Auftraggebers werden grundsätzlich in der Sozietät vor Ort gespeichert oder alternativ im Rechenzentrum der DATEV e.G.

3.1.1. Benutzer- / Rechteverwaltung - Authentifizierung

Die Sozietät hat für alle Benutzer und angelegte Benutzergruppen Rechteprofile angelegt.

1) Rechtevergabe an zugelassene Benutzer

- zu geordnetes Rechteprofil (in Einzelfall mit Abweichungen vom verwendeten Standard Rechteprofil)
- Begründung für die Wahl des Rechteprofils und gegebenenfalls der Abweichungen
- Zuordnung des Benutzers zu einer Organisationeinheit mit Zeitpunkt und Grund der Einrichtung
- Befristung der Einrichtung/ Löschen der Benutzergruppen

2) Rechtevergabe an zugelassene Gruppen

- Zugehörige Benutzer
- Zeitpunkt der Einrichtung
- Befristung der Einrichtung

3.1.2. Zutrittskontrolle

- Das Gebäude ist außerhalb der Arbeitszeit verschlossen.
- Damit sich Besucher zu jeder Zeit anmelden können ist der Empfang während der Arbeitszeiten durchgehend von 08:00 Uhr bis 17:00 Uhr (Freitags von 08:00 Uhr bis 16:00 Uhr) besetzt.
- Wesentliche Räume sind durch eine Alarmanlage gesichert.
- Alle Personen müssen sich am Empfang anmelden. Vor Einlassgewährung wird Rücksprache mit dem Besuchten gehalten. Der Besucher wird am Empfang abgeholt und wird stets von einem Mitarbeiter begleitet.
- Der Zutritt der Räume ist nur speziell autorisierten Mitarbeitern von der Steuerberatersozietät gestattet, die der Verschwiegenheitspflicht gem. § 203 StBG unterliegen bzw. eine entsprechende Verschwiegenheitserklärung unterschrieben haben.
- Die Geschäftsleitung prüft periodisch die Notwendigkeit von Zutrittsberechtigungen für die Mitarbeiter.

3.1.3. Zugangskontrolle

- Zunächst greifen alle Maßnahmen der voran beschriebenen Zutrittskontrolle.
- Alle Rechner (Arbeitsplatz-PC's, Server, Tablets, Smartphones usw.) bei der Sozietät verfügen mindestens über ein Zugangskontrollsystem (UserID, Passwort).
- Zur Prüfung der Wirksamkeit der Absicherungsmaßnahmen werden bei sensiblen Systemen Zeitabständen Penetrationen durchgeführt.
- Arbeitsplatz -PC- Sicherheit :
  Benutzerkennung mit mindestens 4 - stelliger Passwortvergabe. Jeder User bekommt eine eigene Benutzerkennung mit Passwort. (Netzwerk Authentifizierung).
  Automatische passwortgeschützte Bildschirm - und PC-Sperren .

3.1.4. Zugriffskontrolle

Innerhalb des hausinternen Sozietät-Firmennetzwerks werden für verschiedene User unterschiedliche Berechtigungsrollen vergeben. So wird gewährleistet, dass ein Nutzer nur auf solche Verzeichnisse oder Bereiche Berechtigungen erhält, die er auch sehen darf.

Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Systeme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen.

Zusätzlich ist das Sozietäts-Firmennetzwerk in differenzierte hausinterne Netzsegmente eingeteilt. User können folglich nicht auf bestimmte Server zugreifen.

3.1.5. Datenzugriff auf das Rechenzentrum der DATEV e.G.

Der Zugriff erfolgt nur über VPN-Verbindungen.

- Die Datenübertragung zwischen der Sozietät und dem Rechenzentrum der DATEV e.G. bzw. Finanzverwaltung erfolgt grundsätzlich verschlüsselt über eine VPN - Verbindung.
- Auf die Server des DATEV e.G. - Rechenzentrum, im Rahmen der Auftragsverarbeitung, können die Sozietätsmitarbeitern nur über das Sozietäts-Firmennetzwerk zugreifen. Hier werden alle Zugriffe kontinuierlich protokolliert.
- Die IT-Systeme von der Sozietät werden kontinuierlich auf die Wirksamkeit eingesetzter Maßnahmen gegen das Eindringen seitens unbefugter Dritter getestet.

3.1.6. Sicherheitsmaßnahmen bei Fernwartung

Der Aufbau der Fernwartungsverbindung darf nur durch eine von der Geschäftsleitung autorisierte Person erfolgen.

- Ein Dritter darf personenbezogene Daten nur dann vom DV-System der Sozietät herunterladen und auf den eigenen Systemen speichern, wenn zuvor die Erlaubnis der Sozietät erteilt wurde.
- Ein Mitarbeiter der Sozietät ist verpflichtet, die Fernwartungsarbeiten von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.
- Ein Dritter bzw. Auftragsverarbeiter muss personenbezogene Daten, die bei der Fernwartung übermittelt wurden, unverzüglich löschen oder der Sozietät zurückgeben, wenn sie für die Durchführung der Fernwartungsarbeiten nicht mehr erforderlich sind.

3.2. Integrität

Das Risiko materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung ist zu reduzieren Die Integrität ist neben der Verfügbarkeit und Vertraulichkeit eines der drei klassischen Ziele der Informationstechnologie. Die Integrität von Systemen und Diensten erfordert die Absicherung vor Manipulationen

Dazu zählen:

- die Wahrung der referentiellen Sicherheit in Datenbanken die Protokollierung von Änderungen
- das Durchführen von Plausibilitätsprüfungen
- die Verhinderung von der Eingabe von ungültigen Werten
- die Verhinderung der ungewollten Löschung, Überschreibung oder Änderung von Daten

Es ist sicherzustellen, dass Programme und Daten nicht verfälscht und / oder falsche Daten verarbeitet werden, damit sie nicht unbemerkt fehlerhafte Ergebnisse erzeugen oder Funktionen ausführen, die nicht erwünscht sind.

Die Sozietät hat mit den Herstellern der eingesetzten Komponenten des Netzwerkes und den Internet Anbindungs-Providern grundsätzlich Service-Level-Agreements (SLA) geschlossen. Hierbei werden von den Herstellern / Providern laufend bekannte Schwachstellen gemeldet, um geeignete Maßnahmen zur Risikoreduzierung und Fehlerbehebung zu treffen.

Die persönliche Verantwortung jedes Sozietätsmitarbeiters für die Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen wird bei der Sozietät durch Schulungsmaßnahmen und zentral bereitgestellte Informationen gestärkt.

3.2.1. Weitergabekontrolle

Die Sozietät stellt sicher, dass personenbezogene Daten bei der elektronischen Übertragung, beim Transport oder bei der Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder gelöscht worden können.

Sicherung bei der elektronischen Übertragung :

- Bei der elektronischen Übertragung von Auftragnehmerdaten in das Datev e.G. Rechenzentrum sind alle Verbindungen über einen VPN -Tunnel verschlüsselt.
- Die elektronische Übertragung von Auftragnehmerdaten in das Datev e.G.-Rechenzentrum wird protokolliert.

3.2.2. Eingabekontrolle

Maßnahmen zur Gewährleistung der nachträglichen Überprüfung und Nachvollziehbarkeit der Datenverwaltung und -pflege, insbesondere hinsichtlich Eingabe, Veränderung oder Löschung von Daten.

Bei der Erfassung von Kundendaten werden folgende Maßnahmen umgesetzt:

- Die Sozietät erfasst nur Kundendaten, die auftragsrelevant sind.
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle
- Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Erstellung einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

3.2.3. Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten lediglich entsprechend den Weisungen des jeweiligen Auftraggebers verarbeitet werden.

Die Sozietät hat hierzu die folgenden Maßnahmen festgelegt:

- Schriftliche Vereinbarungen und Verträge
- Klare Abgrenzung der Kompetenzen und Pflichten zwischen der Sozietät und Auftraggeber
- Festlegung der Sicherheitsmaßnahmen
- Weisungsbefugnisse eindeutig definiert
- Verpflichtung der Mitarbeiter auf das Datengeheimnis (§ 5 BDSG)
- Vereinbarungen zur Auftragsverarbeitung nach Art. 28 der EU-DSG VO
- Bestellung eines Datenschutzbeauftragten

3.2.4. Trennungskontrolle

Es ist sicher zu stellen, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können.

Stichpunktartig hier die wichtigsten Maßnahmen, die die Sozietät um gesetzt hat:

- Trennung von Produktiv- und Test-System
- Getrennte Ordnerstrukturen (Mandantenfähigkeit)
- Getrennte Tables in der Datenbank
- Getrennte Datenbanken
- Getrennte Server

3.2.5. Löschen von Daten

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es die Zwecke, für die sie verarbeitet werden, erforderlich machen. Die Sozietät hat ein entsprechendes Löschkonzept erarbeitet.

- **Vernichtung von Datenträgern**
  Datenträger werden zentral zwischengelagert und von einem externen Entsorger Datenschutzkonform vernichtet. Die entsprechenden Aufbewahrungsfristen nach dem BGB, HGB, StBG, AO sowie diversen anderen Steuergesetzen werden beachtet.
- **Vernichtung von Schriftstücken**
  Papierbezogene Akten werden nach DIN-66399 bzw. DIN-EN-15713 zertifiziert vernichtet. Die entsprechenden Aufbewahrungsfristen nach dem BGB, HGB, StBG, AO sowie diversen anderen Steuergesetzen werden beachtet.

3.2.6. Mandantentrennung

Zu unter schiedlichen Zwecken erhobene Daten werden getrennt verarbeite, verwaltet.

3.2.7. Protokollierung

Die Verarbeitung von im Auftrag verarbeiteten Daten werden grundsätzlich protokolliert. Die Dateneingabe und die Verarbeitung der im Auftrag verarbeiteten Daten erfolgen ausschließlich nach dem mit den Auftraggebern festgelegten Verfahren.

3.3. Verfügbarkeit

Das Glossar des IT - Grundschutzkataloges des BSI definiert Verfügbarkeit wie folgt:

„Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder TT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können."

Gemeint ist damit die jederzeitige Betriebsbereitschaft von Systemen und Diensten im Sinne der Sicherstellung einer jederzeitigen Nutzbarkeit.

Die Sozietät stellt sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden. Alle Alarmierungspläne, Handlungsanweisungen, Notfallregelungen sind in Notfallhandbuch festgehalten. Die wesentlichen Sicherungsmaßnahmen sind hier stichpunktartig genannt:

- Lüftung im Serverraum
- Unterbrechungsfreie Stromversorgung (USV)
- Zugangskonzept für das Gebäude
- Mehrstufiges Backupkonzept
- RAID Verfahren
- Datenübertragung und Datenspiegelung
- Die Sozietät hält Ersatzgeräte vor bzw. hat mit Herstellern Wartungsverträge mit entsprechenden Service-Level-Agreements (SLA) und kurzen Reaktionszeiten, um bei einem Komponentenausfall umgehend einen Not- bzw. Ersatzbetrieb sicherstellen zu können.
- Das Einspielen von Patches und Hotfixes erfolgt regelmäßig, sobald diese verfügbar sind.

3.4. Zweckbindung

Personenbezogene Daten, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

4. Wiederherstellung

Zur Wiederherstellung der Daten hat die Sozietät folgende Maßnahmen vorbereitet:

- Sicherung der Daten
- Sicherung von Systemdateien und Datencontainern
- Sicherung von LOG-Dateien
- Sicherung von Benutzerkonten

5. Organisatorische Maßnahmen

Eine Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen wird gewährleistet.