Vereinbarung zu den technischen und organisatorischen Maßnahmen

Die folgenden technischen und organisatorischen Maßnahmen werden zwischen dem AUFTRAGGEBER (Verantwortlicher gemäß EU-DSGVO) und dem AUFTRAGNEHMER (Auftragsverarbeiter gemäß EU-DSGVO) Ferber-Software GmbH verbindlich gemäß Artikel 32 Absatz 1 EU-DSGVO festgelegt.

1) Vertraulichkeit - Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen des AUFTRAGNEHMERS, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren:

- Kartengestütztes personalisierte Zugriffskontrollsystem mit Zutrittsberechtigung nur für autorisierte Mitarbeiter.
    - Identifikation per Transponderchip auf Zugangskarte oder Token.
    - Kartenvergabe für neue und Kartenrücknahme von ausscheidenden Mitarbeitern durch das Personalwesen.
    - Sofortige Sperrung bei Verlust einer Karte.
- Organisationsanweisung zur Ausgabe von Schlüsseln zu Mitarbeiterbüros.
    - Abteilungsbezogene Schlüsselkreise.
    - Schlüsselausgabe für neue und Schlüsselrücknahme von ausscheidenden Mitarbeitern durch Personalwesen.
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude.
    - Einlass der Gäste, Vergabe eines Besucherausweises und Sorge für Begleitung durch den Empfang.
    - Dokumentation von: Name des Gastes, Ankunfts- und Abreisezeit sowie besuchtem Mitarbeiter.
- Vergaberichtlinien für Zutrittsberechtigungen zu den Serverräumen.
    - Eigener Schließkreis für die Schlüssel zu den Serverräumen.
    - Bewilligung der Berechtigung zum Erhalt der Schlüssel durch die Geschäftsführung. Schlüsselvergabe durch die zentrale IT.
- Abschließen der einzelnen Büroräume nach Arbeitsschluss.
- Notausgänge
    - Öffnung der Türen von außen nur mit Schlüssel durch hierzu berechtigte Mitarbeiter des AUFTRAGNEHMERS.
- Abschließen des Gebäudes nach Arbeitsschluss.
    - Sicherung des Gebäudes durch eine Alarmanlage.
    - Alarmverfolgung bei aktivierter Alarmanlage durch beauftragten Wachdienst.
    - Dienstzeit des Wachdienstes an Werktagen außerhalb der Geschäftszeiten des AUFTRAGNEHMERS sowie an allen anderen Wochentagen rund um die Uhr.

2) Vertraulichkeit - Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme des AUFTRAGNEHMERS von Unbefugten genutzt werden können:

- Nutzung der Clientsysteme nur nach passwortgestützter Netzwerk-Authentifizierung.
- Administrierung der Serversysteme nur mit Konsolenpasswort oder über passwortgeschützte Verbindung.
- Automatische, passwortgeschützte Bildschirm- und Rechnersperre nach 10 Minuten.
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern, keine unpersönlichen Sammelkonten (z.B. „AZUBIS“):
    - Bewilligung der Benutzerkonten durch die Abteilungsleiter.
    - Einrichtung und Vergabe der Benutzerkonten durch die zentrale IT.
    - Umgehende Deaktivierung von Benutzerkonten ausgeschiedener Mitarbeiter.

    - Keine Administratoren-Berechtigungen für Standard-User.
- Richtlinie „Kennwörter“ zum sicheren, ordnungsgemäßen Umgang mit Passwörtern/Smartcards.
    - Definition von Mindestanforderungen bzgl. der Komplexität von Passwörtern. Verwendung von Zeichen aus drei der folgenden Kategorien:
        Großbuchstaben (A bis Z)
        Kleinbuchstaben (a bis z)
        Zahlen zur Basis 10 (0 bis 9)
        Nicht alphabetische Zeichen (zum Beispiel !, $, #, %)
    - Definition der Länge von Passwörtern (mindestens 12 Zeichen) zur Anmeldung an die Domäne und an Dienstkonten.
    - Automatischer Ablauf von Passwörtern.
    - Absicherung gegen Wiederverwendung von Passwörtern.
    - Die Betriebssystempasswörter sind in Hash-Form gespeichert.
    - Automatisierte Kontosperrung aufgrund von mehreren Kennwort-Fehleingaben
    - Sperrzeit des Kontos nach erfolgter automatisierter Kontosperrung.
    - Mögliche manuelle Kontoentsperrung durch die Administratoren vor Ablauf der automatisierten Kontosperrung

3) Vertraulichkeit - Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems des AUFTRAGNEHMERS 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:

- Methoden zur Datenverschlüsselung: PGP, Bitlocker und AxCrypt.
- Netzlaufwerke mit Zugriff nur für berechtigte Benutzergruppen (s. o.)
- Remote-Zugriff für Mitarbeiter über verschlüsseltes VPN.
- Arbeitsrichtlinien für die Mitarbeiter des AUFTRAGNEHMERS zur Verwendung von mobilen Datenträgern (z. B. Laptop, Wechsel-Festplatten, USB-Sticks) bei Kunden und auf Reisen.
- Verbindliches Verfahren zur Wiederherstellung von Daten aus Backup.
    - Restore durch zentrale IT.
- Betrieb der Antivirensoftware Windows-Defender auf allen Arbeitsplätzen:
    - Tägliche, automatische Updates der Antivirensoftware.
- Durchführung von Software-Updates über zentrale Softwareverteilung.
    - Microsoft Windows Update Services.
    - Microsoft Active Directory Group Policy Extensions.
    - Microsoft System Center Configuration Manager
- Firewallkonzept, welches u. a. den Einsatz von Paketfiltern, IPSs und ALGs beinhaltet.
- SPAM-Filter.
    - Vorabprüfung Nachrichten mit DNS-Blacklisten und Antivirensoftware AMAVIS
    - Ablehnung von SPAM-Nachrichten, Umleitung der SPAM in persönlichen SPAM-Ordner, Prüfung und ggf. Löschung der SPAM durch den Empfänger.
- Verbindliche Richtlinien zum Umgang mit Kundendaten:
    - Nutzung der Kundendaten nur mit expliziter Kundenerlaubnis.
    - Meldung des Eingangs von Kundendaten beim bDSB des AUFTRAGNEHMERS.
    - Festlegung der Frist bis zur Datenlöschung durch den bDSB bzw. durch den Kunden.
    - Kontrolle der Einhaltung der Frist bis zu Datenlöschung sowie Protokollierung der Datenlöschung durch den bDSB des AUFTRAGNEHMERS.
- Zugriffsberechtigungen
    - Bewilligung der Zugriffsberechtigungen durch die Abteilungsleiter
    - Vergabe der Zugriffsberechtigungen durch die zentrale IT.

4) Vertraulichkeit - Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten beim AUFTRAGNEHMER getrennt verarbeitet werden:

- Berechtigungskonzept, das der getrennten Verarbeitung von Daten des AUFTRAGGEBERS von Daten anderer Mandanten Rechnung trägt:
    - Verwendung kundenspezifischer Verzeichnisse.
    - Verwendung kundenspezifischer Datenbanken.
    - Verwendung kundenspezifischer Server/Maschinen.

5) Vertraulichkeit - Pseudonymisierung

Die Verarbeitung personenbezogener Daten, die vom AUFTRAGNEHMER ausschließlich für eigene Zwecke erhoben worden sind, erfolgt in nicht pseudonymisierter Weise entsprechend der jeweiligen Zweckvorgabe.

Sofern personenbezogene Daten von Kunden, Lieferanten oder sonstigen Dritten zur Verarbeitung an Ferber-Software übermittelt worden sind, ist für die Pseudonymisierung dieser personenbezogenen Daten ausschließlich der für die Datenübermittlung Verantwortliche, bei Kunden also der AUFTRAGGEBER, zuständig. Im Rahmen dieser Zuständigkeit ist eine Übertragung der Durchführung der Daten-Pseudonymisierung vom für die Datenübermittlung Verantwortlichen auf Ferber-Software ausdrücklich ausgeschlossen!

6) Integrität - 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:

- Transport von Datenträgern zur externen und von der externen Archivierungsstelle (Bankschließfach) nur durch hierfür befugte Mitarbeiter des AUFTRAGNEHMERS.
- Physische und protokollierte Vernichtung von defekten Datenträgern (z. B. Festplatten, USB-Sticks) oder von Datenträgern, die nicht mehr benötigt werden (z. B. CDs/DVDs), durch Mitarbeiter des AUFTRAGNEHMERS. Eine Protokollierung der Löschung erfolgt durch den AUFTRAGNEHMER.
- Keine Beauftragung externer Dienstleister zur Datenvernichtung.
- Richtlinie für Verschlüsselung von personenbezogenen Daten vor dem Transport.
    - Datenübertragungswege sind vorab mit dem AUFTRAGGEBER abzustimmen.
    - In der Regel per PGP, Bitlocker oder Truecrypt.
    - In Ausnahmen passwortgeschütztes Archiv (falls der AUFTRAGGEBER kein PGP nutzt).
    - Eigene Drucker mit physischer Zugriffskontrolle für den Ausdruck sensibler Daten oder Ausdruck in PIN-geschützte Box.
    - Verwendung von nach Abteilungen getrennten digitalen Fax-Postfächern.

7) Integrität - Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme des AUFTRAGNEHMERS eingegeben, verändert oder entfernt worden sind:

- Vertragliche Beschränkung der Arbeit mit personenbezogenen Daten des AUFTRAGGEBERS auf die im Zusammenhang mit Leistungen aus dem Vertrag tätigen Mitarbeiter des AUFTRAGNEHMERS:

- Initiale Schulung neuer Mitarbeiter durch den bDSB des AUFTRAGNEHMERS.
- Verpflichtung der Mitarbeiter auf das Datengeheimnis gemäß Art. 28 Abs 3 EU-DSGVO, § 35 SGB I, § 78 SGB X, §§ 203, 204 und 206 BGB sowie § 3 TDDDG.
- Regelmäßige Schulungen des Gesamt-Teams bzgl. datenschutzrelevanter Themen durch den bDSB des AUFTRAGNEHMERS.
- Einweisung in kundenspezifische Vereinbarungen / Richtlinien durch den verantwortlichen Projektleiter.

- Registrierung der Benutzer und Uhrzeit der jeweiligen Änderung in Teilnehmer-verwaltungssystemen:
  - Protokollierung von Fernwartungssitzungen inkl. ggf. vorgenommener Änderungen/Löschungen.
  - Werden in Remote-Sitzungen Fernwartungs-Werkzeuge nach Vorgabe des AUFTRAGGEBERS verwendet, ist der AUFTRAGGEBER für die Sitzungsprotokollierung verantwortlich.
  - Elektronisches Änderungslogbuch im CRM-System des AUFTRAGNEHMERS.
  - Elektronisches Änderungslogbuch im Anwendungssystem IKAROS.

8) Verfügbarkeit und Belastbarkeit - Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit beim AUFTRAGNEHMER

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust beim AUFTRAGNEHMER geschützt sind:

- Einsatz einer Festplattenspiegelung.
- Einsatz von Schutzprogrammen:
  - Antivirensoftware Windows-Defender.
  - Firewall.
- Vollständiges Backup- und Recovery-Konzept mit täglicher Sicherung.
  - Aufbewahrung der Datenträger in einem feuerfesten Safe.
  - Zugriff auf diesen Safe nur durch die zentrale IT.
  - Zusätzlich regelmäßige Auslagerung der Sicherungsbänder in ein Bankschließfach.
  - Bedarfsbezogenes Restore (einzelne Dateien, die benötigt werden).
- Einsatz einer unterbrechungsfreien Stromversorgung (USV) für Server.
- Regelmäßige Wartung der Alarmierungs- und Sicherheitssysteme.
- Notfallkonzept für Großschadensereignisse, z. B. Brand
  - Vorbeugende Bereitstellung von CO2-Feuerlöschern bei den zentralen IT-Anlagen.
  - Arbeitsrichtlinien zum Verhalten in Notfällen, z. B. bei einem Brand
  - Durchführung des Alarmplans bei Eintritt von Notfällen
  - Bei Brand Aktivierung der hausinternen Brandmeldeanlage mit Alarmierung des Wachdienstes.
    Außerhalb der Geschäftszeiten des AUFTRAGNEHMERS direkte Alarmierung der Rettungsdienste durch den Wachdienst.
    Während der Geschäftszeiten Alarmierung der Rettungsdienste durch den Wachdienst dann, wenn eine Rückmeldung des AUFTRAGNEHMERS beim Wachdienst nicht innerhalb von 5 Minuten erfolgt ist.
- Kontinuierliche Wartung eingesetzter Soft- und Hardware und Tausch von Betriebsmitteln in nicht kalendarisch festgelegten Abständen bei Bedarf weiterer Kapazität, neuer Funktionen und bei Auftreten höheren Ausfallrisikos.

9) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management

- Dokumentiertes Datenschutzkonzept
- Jährliche Überprüfung der Wirksamkeit der TOM und ggf. Aktualisierung derselben.
- Bestellung von Hr. Ulrich Ewers zum internen Datenschutzbeauftragten (DSB). DSB-Kontaktdaten siehe unten.
- Datenschutzrechtliche Schulung neuer Mitarbeiter mit Abgabe einer Verpflichtungserklärung zum Datenschutz. Ablage derselben in der Personalakte des Mitarbeiters.
- Sensibilisierung der Mitarbeiter durch weitere Unterweisungen, insbesondere bei Aktualisierung der datenschutzrechtlichen Vorgaben.
- Bei Bedarf Durchführung einer Datenschutz-Folgenabschätzung (DSFA).
- Erfüllung der Informationspflichten gemäß Artikel 13 und 14 DSGVO.
- Bearbeitung von Auskunftsanfragen seitens Betroffener durch die jeweilige Fachabteilung, z. B. den Vertrieb oder die Organisation. Ggf. mit Unterstützung durch den DSB.

Vorfall Management

- Einsatz von Firewall, Spamfilter sowie Virenscanner und deren regelmäßige Aktualisierung.
- Meldung von Sicherheitsvorfällen oder Datenpannen durch den DSB innerhalb der in der Vereinbarung zur Auftragsverarbeitung definierten Fristen und an die dort benannten Stellen.
- Somit Einbindung des DSB in Sicherheitsvorfälle oder Datenpannen.
- Dokumentation von Sicherheitsvorfällen oder Datenpannen.
- Nachbearbeitung von Sicherheitsfällen oder Datenpannen (Leiter der betroffenen Fachabteilung, DSB und Geschäftsführung).
- Ggf. Aufstellung weiterer Arbeitsrichtlinien zur zukünftigen Verhinderung der aufgetretenen Sicherheitsfälle oder Datenpannen.
- Unterweisung aller Mitarbeiter in die neuen oder erweiterten Arbeitsrichtlinien.

Datenschutzfreundliche Voreinstellungen

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.
- Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen, z. B. einer anzuhakenden Kontrollbox im Kontaktformular.

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des AUFTRAGGEBERS verarbeitet werden:

- Vertragliche Festlegung von Art und Umfang sowie Zweck der beauftragten Verarbeitung und Nutzung personenbezogener Daten des AUFTRAGGEBERS.
- Auf Wunsch Benennung verantwortlicher Personen des AUFTRAGGEBERS, die in Bezug auf die vereinbarte Auftragsdatenverarbeitung gegenüber dem AUFTRAGNEHMER weisungsbefugt sind.
- Einbindung des DSB des AUFTRAGNEHMERS in die dafür relevanten betrieblichen Prozesse.
- Bei Terminen vor Ort in den Räumen des Kunden Kontrolle durch Mitarbeiter des AUFTRAGGEBERS.
- Regelungen für Mitarbeiter des AUFTRAGNEHMERS zum Arbeiten per Mobile Working.
- Regelung zum Einsatz von Subunternehmen.
- Verpflichtung der Subdienstleister des AUFTRAGNEHMERS zur Einhaltung der EU-DSGVO.
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.

Innerbetrieblicher Datenschutzbeauftragter des AUFTRAGNEHMERS

Nach Maßgabe des Artikels 37 EU-DSGVO bzw. § 38, Abs. 1 BDSG ist beim AUFTRAGNEHMER Herr Ulrich Ewers, datenschutz@ferber-software.de, zum innerbetrieblichen Datenschutzbeauftragten bestellt worden.
Herr Ewers ist telefonisch zu erreichen unter der Nummer +49 2941 9665-100, per Fax unter der Nummer +49 2941 9665-409.

Zusammenfassung

Neben diesen technischen und organisatorischen Maßnahmen hat der Datenschutzbeauftragte des AUFTRAGNEHMERS eine Reihe weiterer Arbeitsrichtlinien zum Datenschutz und zur Datensicherheit erlassen. Gemeinsam mit den Leitern der einzelnen Fachabteilungen der Ferber-Software GmbH wird die Einhaltung dieser Richtlinien überwacht und bei Bedarf eine Modifizierung bestehender oder eine Neuanlage von Arbeitsrichtlinien vorgenommen.
Neue Mitarbeiter der Ferber-Software GmbH werden durch persönliche Datenschutz-unterweisungen in das firmeninterne Regelwerk eingewiesen. Auffrischungsschulungen werden jährlich durchgeführt. Ein besonderes Augenmerk wird dabei auf das Erkennen von Datenschutzvorfällen gelegt.
Die bei Vorlage der Voraussetzungen des Artikels 33 EU-DSGVO vom AUFTRAGNEHMER zu treffenden Maßnahmen werden in den mit dem jeweiligen AUFTRAGGEBER abgeschlossenen AV-Verträgen definiert. Bei der Verarbeitung von Daten für eigene Zwecke erfolgt eine Meldung an die Aufsichtsbehörden innerhalb von 72 Stunden nach Kenntniserlangung von dem Vorfall.