Dokumentation der technischen und organisatorischen Maßnahmen zur Datensicherheit gem. Art. 30 Abs. 1 lit. g i.V. m. Art. 32 Abs. 1 DS-GVO

Inhalt

Einleitung

Jedes Unternehmen ist verpflichtet, im Rahmen der Erhebung sowie der Be- und Verarbeitung personenbezogener Daten gem. Unternehmenszweck für eine ausreichende Datensicherheit als Grundvoraussetzung für den Datenschutz Sorge zu tragen. Das Grundkonzept zur Datensicherheit ist seitens des Gesetzgebers durch die sog. technischen und organisatorischen Maßnahmen zur Datensicherheit gem. Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO vorgegeben.

Gleichzeitig gilt das Konzept im Rahmen der Vergabe von Auftragsdatenverarbeitung nach Art. 28 DS-GVO als Nachweis bei der Bewertung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen und wird Vertragsgegenstand bei Vertragsabschluss.

Die KMH GmbH ist ein Softwareentwicklungsunternehmen, welches durch unterschiedlich ausgestaltete Auftragsverhältnisse über verschiedenste systemische Wege auf personenbezogene Daten Zugriff erhält und diese teils im Sinne der DS-GVO verarbeitet. Hierzu wird im Folgenden an entsprechend notwendiger Stelle zwischen internen Systemen, cloudbasierten Systemen und Fremdsystemen differenziert.

Definition der unterschiedlichen Systeme:

1. **Interne Systeme** – unter diese Begrifflichkeit fallen bspw. alle Firmenlaptops, internen Netzwerke und Telefoniegeräte.

2. **Cloudbasierte Systeme** – unter diese Begrifflichkeit fallen alle cloudbasierten Systeme, die intern verwaltet werden. Somit alle Systeme, die in einer Cloud gehostet werden und bei denen die KMH GmbH Vertragspartner und somit Root-Admin ist.

3. **Fremdsysteme** – unter diese Begrifflichkeit fallen alle extern verwalteten Systeme. Hierunter fallen alle in einer Cloud oder in anderweitigen Rechenzentren gehosteten Systeme, auf die die KMH GmbH zugreifen kann, welche jedoch extern verwaltet werden.

Im Folgenden sind die technisch-organisatorischen Maßnahmen der KMH GmbH nach diesen Maßgaben aufgeführt und erläutert:

Verantwortliche Stelle:

KMH GmbH
Zollstockgürtel 61
50959 Köln

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

Technisch-organisatorische Maßnahmen

- Elektronische Schließanlage (Winkhaus Blue Chip Schlüssel) – vom Vermieter gestellt und jeder Schlüssel gesondert bestellt und aktiviert, Sicherheitsschlösser, Sicherheitsglas.
- Schlüsselausgabeprotokoll.
- Protokollierung der Besucher.
- Besucherregelung: Jeder externe Besucher wird von einem internen Mitarbeiter während des gesamten Besuches in den Geschäftsräumen begleitet.
- Rauchalarm, Brandalarm.
- Alle Mitarbeiter unterliegen einer Homeoffice Richtlinie.

1.2 Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technisch-organisatorische Maßnahmen

In allen folgenden System werden Passwörter ausschließlich in einem zentralen cloudbasierten Passwortmanager (Keeper Security Inc.) verwaltet. Jeder Mitarbeiter verfügt über einen persönlichen Passwortbereich und einen je nach Berechtigung freigegebenen Unternehmensbereich. Der persönliche Passwortbereich kann nur von dem Mitarbeiter selbst eingesehen und verwaltet werden. Der Passwortmanager generiert besonders sichere Passwörter, welche durch die Mitarbeiter zu verwenden sind.

Interne Systeme

1.2.1 Netzwerk

- Firmennetzwerk über Firewall vor Fremdzugriff geschützt.

- WLAN ist stets mit einer Verschlüsselungstechnologie mit Passwort gemäß den aktuellen technischen Richtlinien des BSI gesichert.

1.2.2 Firmenlaptops

- Jeder Mitarbeiter besitzt einen Firmenlaptop auf dem Administratorberechtigungen vorhanden sind.
- BIOS-Passwort: das BIOS ist mit einem Passwort geschützt und das Booten über externe Geräte ist über das gleiche Passwort geschützt.
- Die Mitarbeiter sind verpflichtet, die Anmeldung am Betriebssystem durch eine der gängigen Authentifizierungsmethoden abzusichern (Passwort, Pin, Biometrisches Verfahren).
- Die Weitergabe von persönlichen Zugängen und Passwörtern ist streng untersagt.
- Alle Mitarbeiter sind verpflichtet, den Firmenlaptop bei Verlassen zu sperren.

1.2.3 Telefoniegeräte

Alle Mitarbeiter unterzeichnen eine gesonderte Vereinbarung „Vereinbarung über die Überlassung und Nutzung eines Mobiltelefons“ und verpflichten sich zur Einhaltung der dortigen Bestimmungen mitunter:

- Die Mitarbeiter sind verpflichtet, die Anmeldung am Mobiltelefon durch eine der gängigen Authentifizierungsmethoden abzusichern (mindestens Code Sperre; je nach Handymodell Fingerabdruck Scan oder Face Scan oder sonstige mögliche Sicherheitseinstellungen).

Cloudbasierte Systeme

- Für sämtliche Clouddienste existieren personalisierte durch Passwörter geschützte Benutzerkonten. Sofern technisch möglich wird eine 2-Faktor-Authentifizierung verwendet. Die Zugangs- und Zugriffsrechte auf Clouddienste werden ausschließlich von jeweilig berechtigten IT-Mitarbeitern (Administratoren) eingerichtet und dokumentiert.
- Es existiert eine cloudbasierte Verzeichnisstruktur (OneDrive). Die Zugangs- und Zugriffsrechte auf die Verzeichnisstruktur werden ausschließlich von jeweilig berechtigten IT-Mitarbeitern (Administratoren) eingerichtet und dokumentiert.

Fremdsysteme

Die KMH GmbH entwickelt für Ihre Auftraggeber Softwareprodukte, welche bei Bedarf auch innerhalb der Infrastruktur des Auftraggebers gehostet und betrieben werden. Die KMH GmbH erhält hierfür die notwendigen Zugriffsrechte vom Auftraggeber.

- Wenn möglich wird eine Multifaktor-Authentifizierung verwendet.
- Passwörter der personalisierten Accounts werden im persönlichen Bereich von Keeper Security Inc. gespeichert.
- Der Zugang zur Infrastruktur von externen Dienstleistern oder Kundensystemen erfolgt über ein gesichertes VPN oder über SSH oder über personalisierte Accounts.

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems 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.

Technisch-organisatorische Maßnahmen

Interne Systeme

- Alle Arten von voreingestellten Hersteller-Passwörtern werden sofort geändert (das betrifft neben Softwaresystemen auch Hardware, wie z.B. Router oder Firewall-Systeme). Die Passwörter sind gemäß Zugangskontrolle im entsprechenden Passwortmanager zu speichern. (s.o.)
- Bei Abwesenheit sind alle IT-Systeme vor Unbefugten durch Sperren der Anwendung, ordnungsgemäßes Abmelden oder durch Aktivierung eines Bildschirmschoners/ Screenlock mit Passwortschutz zu schützen.
- Festplatten der Dienstlaptops sind verschlüsselt (aktuell Bitlocker oder vergleichbare Verschlüsselung)

Cloudbasierte Systeme

- Es existiert eine gemeinsam genutzte Verzeichnisstruktur. Diese ist mit individuellen Rechten versehen. Die Rechtevergabe erfolgt ausschließlich von (der Geschäftsführung) definierten Mitarbeitern. Jeder Mitarbeiter hat nur die Berechtigung, die er zwingend benötigt.
- Vergabe und Änderung von Zugriffsberechtigungen dürfen nur nach expliziter Freigabe des Vorgesetzten durch die hierfür berechtigten Mitarbeiter erfolgen.
- Für die Administration der cloudbasierten System darf lediglich der persönliche Administrations-Account verwendet werden, der allgemeine Administrator-Account bzw. das allgemeine Root-Passwort darf nur im Notfall verwendet werden oder wenn es nicht anders möglich ist.

Fremdsysteme

- Mitarbeiter werden nur mit Zugriffsrechten ausgestattet, die unmittelbar für die Erledigung ihrer Aufgaben vorgesehen sind.
- Vergabe und Änderung von Zugriffsberechtigungen dürfen nur von definierten Mitarbeitern erfolgen.
- Für den Zugriff auf Fremdsysteme darf lediglich ein persönlicher Zugang verwendet werden, der allgemeine Administrator-Account bzw. das allgemeine Root-Passwort darf nur im Notfall verwendet werden oder wenn es nicht anders möglich ist.
- Ein Fernzugriff (Remote) erfolgt ausschließlich über eine gesicherte Verbindung.

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technisch-organisatorische Maßnahmen

Folgende Maßnahmen zur Trennungskontrolle wurden getroffen:

- Logische Mandantentrennung.
- Berechtigungskonzept.

  - Funktionstrennungen, Trennung durch Zugriffsregelungen.
- Trennung Produktiv- und Testsystem.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO) und Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes 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:

Technisch-organisatorische Maßnahmen

Eine Weitergabe von vertraulichen Informationen bedarf der Zustimmung des Informationseigentümers. Bei der Weitergabe von personenbezogenen Daten ist ihr Schutzbedarf zu beachten und eine geeignete Versandart zu wählen.

Folgende Maßnahmen zur Weitergabekontrolle wurden getroffen:

- Alle Mitarbeiter sind schriftlich zur Wahrung der Vertraulichkeits- und Datenschutzvorschriften (Datengeheimnis) und das Fernmeldegeheimnis verpflichtet.
- Austausch von vertraulichen Dokumenten über SFTP oder verschlüsselte ZIP-Dateien.
- Getunnelte Datenfernverbindungen (VPN = Virtual Private Network).
- Gesichertes WLAN.
- SSL-Verschlüsselung bei Web Access.
- Einsatz von Aktenvernichtern.
- Ggf. erforderliche Weitergabe von Daten in anonymisierter oder pseudonymisierter Form.
- Eine notwendige Vernichtung von Datenträgern erfolgt durch ein spezialisiertes und zertifiziertes Unternehmen nach aktuellen Normen.
- Pseudonymisierung.

2.2 Eingabekontrolle

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

Technisch-organisatorische Maßnahmen

Folgende Maßnahmen zur Eingabekontrolle wurden getroffen:

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts.
- Systemseitige Protokollierungen.

- Festlegung von funktionellen Verantwortlichkeiten.
- Alle Tätigkeiten (Speicherung, Löschen, Übertragen, Verarbeiten, Konfigurieren)
  - an/auf Systeme mit personenbezogenen Daten oder
  - mit Zugriff auf personenbezogene Daten

  werden nach Person, Art, Inhalt und Zeitpunkt protokolliert. Nach Möglichkeit ist immer das Mehr-Augen-Prinzip anzuwenden.
- Eine Auswertung der Eingabekontrolle erfolgt nur bei Bedarf im Rahmen der Weisung durch eine manuelle oder automatisierte Protokollauswertung.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO) und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind.

Technisch-organisatorische Maßnahmen

Folgende Maßnahmen zur Verfügbarkeitskontrolle wurden getroffen:

Interne Systeme

- Mitarbeiter dürfen keine eigenen oder zur Verfügung gestellten Geräte als Speicherort für personenbezogene Daten nutzen (Server siehe unten: Fremdsysteme).
- Backup- & Recoverykonzept (Fileserver).
- Das Betriebssystem ist mit aktueller Antivirensoftware sowie einer Firewall Software geschützt.
- Die Betriebssysteme und Anwendungen werden regelmäßig mit den aktuellsten Sicherheitsupdates versehen.
- Es werden nur Betriebssysteme und Anwendungen verwendet, die noch Herstellersupport beinhalten.
- Definierte Meldewege.
- Automatische Schließanlage an den Eingangstüren des Bürogebäudes.
- Sicherheitsdienst mit Sicherheitsüberwachung.
- Feuer- und Rauchmeldeanlagen.

Cloudbasierte Systeme und Fremdsysteme

Daten auf cloudbasierten Systemen und Fremdsystemen sind gemäß dem Standard des Cloudanbieters, des Auftraggebers oder des Rechenzentrums-Dienstleisters vor Ausfall geschützt. Es existieren entsprechende Vereinbarungen bezüglich der Verfügbarkeit mit allen Anbietern/Dienstleistern.

Folgende Maßnahmen sind in diesem Zusammenhang als Standard anzusehen:

- Backup- & Recoverykonzept (Fileserver).
- Betriebssysteme sind mit aktueller Antivirensoftware sowie einer Firewall Software geschützt.
- Die Betriebssysteme werden regelmäßig mit den aktuellsten Sicherheitsupdates versehen.
- Es werden nur Betriebssysteme verwendet, die noch Herstellersupport beinhalten.
- Definierte Meldewege.
- Unterbrechungsfreie Stromversorgung (USV).
- Speichertechnologie: RAID-System; Sicherungskopien.
- Feuer- und Rauchmeldeanlagen.
- Klimaanlage.
- Alarmanlage.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1 Datenschutz-Management

- Datenschutzorganisation und Verteilung der Verantwortlichkeiten.
- Datenschutzrichtlinien.
- Datenschutz-Koordinatoren.
- Verpflichtung auf das Datengeheimnis / Vertraulichkeit und das Fernmeldegeheimnis.
- Datenschutz-Schulung / Sensibilisierung der Mitarbeiter.
- Einbindung des Datenschutzbeauftragten bei:
  - Beschwerden von Betroffenen (Mitarbeitern, Kunden).
  - Einführung eines neuen Systems / Tools, Einsatz neuer Technologien.
  - Einsatz eines neuen Dienstleisters.
  - Werbemaßnahmen (z.B. Versand von Newsletter).
  - Onlinemarketing-Maßnahmen (Google AdWords, Conversion Tracking, etc.).
  - Verkauf von Teilen des Unternehmens.
  - Wenn ein hohes Risiko für Rechte und Freiheiten von Personen vermutet wird.
  - Bei systematischer und umfassender Bewertung persönlicher Aspekte, auch Profiling.
  - Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.
  - Bei umfangreicher Verarbeitung besonderer Kategorien personenbezogener Daten.

4.2 Incident-Response-Management

Maßnahmen, um nach einem physischen oder technischen Zwischenfall die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen rasch wiederherzustellen.

Im Rahmen des etablierten BCM (Business Continuity Management) zur Sicherstellung des Geschäftsbetriebes während einer Notlage oder Großstörung sowie zur schnellstmöglichen Wiederherstellung aller für den Auftraggeber bereitzustellenden Dienste sind Verfahren dokumentiert.

Maßnahmen rund um die Speicher-, Zugriffs- und Leitungskapazitäten, sowie zu Backup und Redundanz-Konzepten sind in der Verfügbarkeitskontrolle detaillierter aufgenommen.

Definierter Prozess bei Datenpannen und IT-Sicherheitsvorfällen.

4.3 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 DSGVO

Technisch-organisatorische Maßnahmen

- Trennung der Daten nach Verarbeitungszweck.
- Nur erforderliche Daten verarbeiten.
- Zugriffsschutz per Voreinstellung.
- Anonymisierung und Pseudonymisierung der Daten.
- Transparenz durch Dokumentation.
- Verschlüsselte Kommunikation.

4.4 Auftragskontrolle

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

Technisch-organisatorische Maßnahmen

Folgende Maßnahmen zur Auftragskontrolle wurden getroffen:

- Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers.
- Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.
- Schriftlicher Vertrag zur Auftragsdatenverarbeitung gem. Art. 28 DS-GVO mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers.
- Verpflichtung der Mitarbeiter auf das Datengeheimnis / Vertraulichkeit und das Fernmeldegeheimnis.
- Schulungen aller zugriffsberechtigten Mitarbeiter, regelmäßig stattfindende Nachschulungen.
- Datenschutzaudits durch den Datenschutzbeauftragten.
- Bestimmung von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag.