Anlage „Technische und organisatorische Maßnahmen“

Generelle Beschreibung

- Vorhandensein von internem IT-Sicherheitskonzept und IT-Sicherheitsrichtlinien.
- Fremdfirmen haben keinen Zugriff auf Datenverarbeitung.
- Vertretungsregelung für IT-Verantwortlichen bei Urlaub oder Krankheit.
- Keine Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DSGVO.
- Schriftliche Bestellung eines Datenschutzbeauftragten.
- Verpflichtung aller Mitarbeiter nachweislich auf das Datengeheimnis sowie ggf. § 88 TKG und ggf. § 35 SGB I, Belehrung über den § 203 StGB.
- Regelmäßige Kontrolle bzgl. Einhaltung von Datenschutz- und Datensicherheitsmaßnahmen.
- Vorhandensein von Verzeichnissen von Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DSGVO, soweit eine Verpflichtung gem. Art. 30 Abs. 5 DSGVO besteht.
- Namentliche Nennung der Ansprechpartner (IT/DV-Verantwortlicher und externer Datenschutzbeauftragter) zur Klärung fachlicher, technischer und organisatorischer Fragen.
- Rechenzentrum: Terra Cloud WORTMANN AG Bredenhop 20 32609 Hüllhorst
- Pseudonymisierung der Daten, soweit dies unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen in Anbetracht der Verarbeitungszwecke möglich ist.
- Verschlüsselung der Daten, soweit dies unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen in Anbetracht der Verarbeitungszwecke möglich ist.

In den folgenden Abschnitten sind einige technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO konkret beschrieben:

1. Zugangskontrolle

Die Zugangskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt (physikalische Sicherheit) zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen im Einzelnen:

- Aufgrund der Lage der Geschäftsräume sind Einwirkversuche von außen über die Fenster ausreichend verhindert. Die Geschäftsräume sind nur durch Personal mit entsprechenden Transpondern oder Shlüsseln zu betreten.
- Zusätzlich werden außerhalb der Bürozeiten einbruch- und feuerhemmende Sicherheitstüren verschlossen.
- Ausgabe und Rückgabe von Transpondern und Schlüsseln ist geregelt.
- Betriebsfremde Besucher werden am Empfang begrüßt, stets von Mitarbeitern des Auftragnehmers begleitet und können sich nicht unkontrolliert im Bürobereich aufhalten.
- Der Auftragnehmer verpflichtet auch weitere Auftragnehmer, die keinen Kontakt zur Datenverarbeitung haben (beispielsweise den Gebäudereiniger), die eigenen Mitarbeiter über den Datenschutz aufzuklären und diese aufzufordern, sich vorsichtig zu verhalten, insbesondere Schlüssel sorgfältig zu verwahren.
- Personen, die nicht für die Wartung und den Betrieb der Server zuständig sind, erhalten keinen Zutritt zu den Serverräumen.
- Videoüberwachung des Eingangsbereiches und der Innenräume ausserhalb der Geschäftszeiten

2. Datenträgerkontrolle
Die Datenträgerkontrolle umfasst Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen (logische Sicherheit) durch Unbefugte verhindert wird.
Maßnahmen im Einzelnen:
- Externer Zugriff von den Mitarbeitern des Auftragnehmers auf den Server des Auftragnehmers ist nur via VPN und Authentifizierung am Auftragnehmer-LAN möglich.
- Trennung Gast-WLAN vom Firmennetzwerk.
- Auftragnehmer-WLAN wird mit WPA2 betrieben.
- Anti-Viren-Software auf allen eingesetzten IT/DV-Anlagen.
- Akten unter Verschluss. Zugang nur für berechtigte Personen.
- Der Zugang zu den IT-Systemen ist durch Zugangsberechtigungen geregelt. Eine Firewall verhindert ungewollte Zugriffe von außen.
- Werden Passwörter mehrfach fehlerhaft eingegeben, erfolgt eine Sperrung. Diese kann nur durch einen Administrator rückgängig gemacht werden.
- Die Mitarbeiter sind gehalten, Notebooks vor unberechtigtem Zugriff zu schützen und so wenig Daten wie möglich aus dem Bereich des Auftraggebers auf dem Notebook zu speichern (sondern möglichst nur innerhalb der zentralen Server vom Auftragnehmer).
- Wenn ein Mitarbeiter ausscheidet, gibt er die ihm zur Verfügung gestellten Geräte an den Auftragnehmer zurück.

3. Speicherkontrolle
Die Speicherkontrolle umfasst Maßnahmen, mit denen die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten verhindert wird.
Maßnahmen im Einzelnen:
- Zugriffe auf die Server des Auftragnehmers erfolgen durch Authentifizierung (Benutzername/Passwort) mit entsprechenden Zugriffsberechtigungen.
- Über Zugriffsberechtigungen wird außerdem sichergestellt, dass die Mitarbeiter nur auf die Datenbanken, Anwendungen und Daten zugreifen können, die sie für ihre Aufgabenerfüllung benötigen.
- Bei Zugriff auf Daten beim Auftraggeber ist durch die vom Auftragnehmer eingesetzte Fernwartungssoftware sichergestellt, dass berechtigte Mitarbeiter des Auftragnehmers ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass alle Zugriffe in der Kundendokumentation festgehalten werden.
- Wenn ein Mitarbeiter ausscheidet, werden ihm die Zugriffsrechte entzogen.
- Die Datenfernübertragungssysteme des Auftragnehmers sind mit Datenverschlüsselung versehen und werden auf dem jeweils aktuellen technischen Stand gehalten.
- Aufgrund der aufgeführten Maßnahmen ist es Unbefugten nicht möglich, Daten aus dem Auftraggeberbereich zu lesen, zu kopieren, zu ändern oder zu entfernen.
- Wenn der Auftragnehmer die Daten aus dem Auftraggeberbereich nicht mehr benötigt, werden die Datenträger nach DIN-Norm 66399 und gemäß den Bestimmungen des Datenschutzes vernichtet. Eventuell angefertigte Kopien der Daten, die zum Zweck der Aufgabenerfüllung erstellt wurden, werden gelöscht.
- Siehe im Übrigen Datenträgerkontrolle und Zugriffskontrolle.

4. Benutzerkontrolle
Die Benutzerkontrolle umfasst Maßnahmen, mit denen die Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte verhindert wird.
Maßnahmen im Einzelnen:
- Siehe Datenträgerkontrolle und Zugriffskontrolle.

5. Zugriffskontrolle
Die Zugriffskontrolle umfasst Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.
Maßnahmen im Einzelnen:
- Vorhandensein eines Berechtigungskonzepts.
- Vorhandensein eines Datensicherungskonzeptes
- Datensicherungen werden verschlüsselt.
- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Verbot der Nutzung privater Datenträger.
- Zugriff auf Notebooks, PC und Server vom Auftragnehmer nur mit Username und Passwort möglich.
- Passwörter unterliegen definierten Passwortrichtlinien (hohen Anforderungen).
- Administratoren sind für Vergabe und regelmäßige Änderung von Passwörtern verantwortlich.
- Zugangsprotokollierung.
- Sperrung nach mehrmaligen fehlerhaften Anmeldeversuchen, Zugriffsversuche werden protokolliert
- Vernichtung ausgedruckter Daten im Aktenvernichter bzw. durch zugelassene Fachunternehmen.
- Umgang mit Datenträgern sowie Verwendung von USB-Sticks, PDAs, externen Festplatten, Tablets und Smartphones und anderer externer Geräte durch Arbeitsanweisung schriftlich geregelt.
- gruppenweiter Auto-Logout nach definierter Zeitspanne der Inaktivität

6. Übertragungskontrolle
Die Übertragungskontrolle umfasst Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.
Maßnahmen im Einzelnen:
- Der Auftragnehmer bearbeitet die Daten nur im Rahmen der Weisungen des Auftraggebers.
- Die Speicherung von Daten aus dem Auftraggeberbereich erfolgt nur während der Arbeiten zur Mängelbeseitigung oder zur Unterstützung des Einsatzes der vom Auftragnehmer gelieferten Systeme bzw. von Systemen, für die der Auftragnehmer Serviceleistungen erbringt. Daten aus dem Bereich des Auftraggebers werden an einen Dritten nur weitergegeben, sofern der Auftraggeber das im Einzelfall schriftlich wünscht.
- Der Auftraggeber kann dem Auftragnehmer die Daten entweder verschlüsselt über eine gesicherte Fernwartungsverbindung auf einen Server des Auftragnehmers übertragen oder als Datenbank auf einem Datenträger zur Verfügung stellen.

7. Eingabekontrolle
Die Eingabekontrolle umfasst Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder aus diesen entfernt worden sind.
Maßnahmen im Einzelnen:
- Regelungen zur Dateneingabe sind vorhanden.
- Erstellung und Änderung von Daten wird protokolliert.
- Es ist nicht vorgesehen, dass der Auftragnehmer personenbezogene Daten aus dem Bereich des Auftraggebers in die Software eingibt.
- Werden personenbezogene Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche an den Auftragnehmer übertragen, werden diese Daten nach Beendigung der Fehlersuche gelöscht. Eine Veränderung oder Entfernung im Sinne des Datenschutzrechts findet nicht statt, es sei denn, dass der Auftraggeber dies vorher ausdrücklich schriftlich beauftragt hat.

8. Transportkontrolle
Die Transportkontrolle umfasst 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.
Maßnahmen im Einzelnen:
- Firewall.
- Versendung personenbezogener Daten mit verschlüsselter elektronischer Verbindung.
- Statistiken mit personenbezogenen Inhalten werden nur im Auftrag von Auftraggeber und nur an berechtigte Personen bei Auftraggeber übermittelt.
- bei physikalischen Versand von Datenträgern mit pbD werden ausschließlich zertifizierte Dienstleister eingesetzt

9. Wiederherstellbarkeit
Die Wiederherstellbarkeit umfasst Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.
Maßnahmen im Einzelnen:
- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Datenträgerverwaltung, Datensicherung, Aufbewahrung außerhalb des Gebäudes.
- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Dokumentation von Datenträgerwechseln und Aufbewahrungsorten.

10. Zuverlässigkeit
Die Zuverlässigkeit umfasst Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.
Maßnahmen im Einzelnen:
- Siehe Verfügbarkeitskontrolle.

11. Datenintegrität
Die Datenintegrität umfasst Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.
Maßnahmen im Einzelnen:
- Siehe Verfügbarkeitskontrolle.

12. Auftragskontrolle
Die Auftragskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen verarbeitet werden können.
Maßnahmen im Einzelnen:
- Alle Mitarbeiter des Auftragnehmers sind angewiesen, nur nach den vereinbarten Vertragsinhalten zu arbeiten.
- Weitergabe personenbezogener Daten erfolgt nur nach schriftlicher Einwilligung oder aufgrund gesetzlicher Bestimmungen.
- Dienstleister des Auftragnehmers unterliegen Überprüfungen.
- Der Auftragnehmer führt Arbeiten, bei denen er Kontakt zu personenbezogenen Daten aus dem Bereich des Auftraggebers bekommen kann oder bekommen soll, nur durch, wenn dieser diese im Einzelfall anfordert. Dies ist beispielsweise dann der Fall, wenn der Auftraggeber an den Auftragnehmer einen Fehler oder ein Problem meldet.
- Alle Mitarbeiter des Auftragnehmers, die mit personenbezogenen Daten aus dem Bereich des Auftraggebers in Kontakt kommen können, sind schriftlich auf die Einhaltung des Datenschutzes verpflichtet. Sie sind entsprechend belehrt und angewiesen, dass sie Arbeiten gemäß dem vorstehenden Absatz nur auf Anforderung des Auftraggebers durchführen dürfen.

13. Verfügbarkeitskontrolle
Die Verfügbarkeitskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
Maßnahmen im Einzelnen:
- Tägliche Datensicherung.
- Feuerlöscher in ausreichender Anzahl im Gebäude.
- Brandschutztüren.
- Vorgaben des Brandschutzes werden eingehalten.
- Serverraum mit unterbrechungsfreier Stromversorgung, Überspannungsschutz.
- Back-Up-Verfahren für Server.
- Alle betroffenen Server verfügen über RAID-Systeme, welche das Verlustrisiko minimieren.
- Sicherungskopien außerhalb des Gebäudes.
- Klimatisierte Cloud-Struktur zum Schutz vor Überhitzung bei Dienstleister (Wortmann Cloud)
- Virenschutzprogramme auf allen Computersystemen.
- Der Auftragnehmer setzt eine Firewall und aktuelle Virenscanner zur Absicherung sowohl des zentralen Datenbankservers als auch des E-Mail-Servers ein. Die Virensignaturen des verwendeten Virenscanners werden täglich mehrmals aktualisiert.
- Arbeitsplatzrechner werden laufend durch aktuelle Scannerprogramme auf Schadsoftware, Malware überprüft. E-Mail-Anhänge werden auf Infizierung überwacht.
- Die Mitarbeiter sind verpflichtet, personenbezogene Daten, die sie auf ihren Notebooks gespeichert haben, möglichst bald auf ein zentrales System des Auftragnehmers zu überspielen.
- Notfallplan.

14. Trennbarkeit
Das Trennungsgebot umfasst Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
Maßnahmen im Einzelnen:
- Wenn Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche oder deren Wiederherstellung übertragen werden, werden diese gesondert von Daten anderer Auftraggeber gespeichert.