Technische und organisatorische Maßnahmen

der Bornemann AG

04.01.2021

V 0.3

Technische und organisatorische Maßnahmen

Änderungshistorie

Versionsnummer	Vorgenommene Änderung	Änderungsdatum	Kürzel d. Mitarbeiters
V 0.1	Erstellung der technischen und organisatorischen Maßnahmen	14.03.2016	NIE
V 0.2	Überarbeitung der kompletten technischen und organisatorischen Maßnahmen	28.07.2020	WDU
V 0.3	Aktualisierung der technischen und organisatorischen Maßnahmen	04.01.2021	ULZ

Technische und organisatorische Maßnahmen

Definitionen

Auftraggeber
Bei dem Auftraggeber im Sinne des Vertrages über die Verarbeitung personenbezogener Daten gemäß Art. 28 DS-GVO handelt es sich um den Kunden.

Auftragnehmer
Bei dem Auftragnehmer im Sinne des Vertrages über die Verarbeitung personenbezogener Daten gemäß Art. 28 DS-GVO handelt es sich um die Bornemann AG.

Zutrittskontrolle
Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Zugangskontrolle
Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Zugriffskontrolle
Es ist zu 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.

Trennungskontrolle
Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Weitergabekontrolle
Es ist zu 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 welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Eingabekontrolle
Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Auftragskontrolle
Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Verfügbarkeitskontrolle
Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

01. Zutrittskontrolle

In den Niederlassungen der Bornemann AG sind die Türen und Tore der Gebäude mit Sicherheitsschlössern versehen. Türen und Fenster sind außerhalb der Betriebszeiten fest verschlossen.

Außerhalb der Betriebszeiten erfolgt eine Überwachung der Liegenschaften und der darauf befindlichen Gebäude mittels Videokameras, die außerhalb und innerhalb der Gebäude installiert sind. Die Videokameras verfügen über eine Motion-Detection-Funktion, mittels derer bei definierten Anlassarten (z.B. Perimeterschutz, Linienüberquerung, Einbruchserkennung usw.) eine Alarmmeldung an einen hierfür autorisierten Personenkreis versendet wird. Dieser Personenkreis kann per Fernzugriff auf die Livebilddateien der Videokameras zugreifen, die aktuelle Situation prüfen und ggf. Sicherheitskräfte informieren.

Zudem werden die Liegenschaften und Gebäude der Bornemann AG außerhalb der Betriebszeiten mehrfach in unregelmäßigen Abständen durch einen privaten Sicherheitsdienst bestreift und kontrolliert.

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

a. Festlegung befugter Personen
b. Vorhandensein von Regelungen für Firmenfremde
c. Durchführung von Anwesenheitsaufzeichnungen
d. Sicherung der Liegenschaften und Gebäude außerhalb der Betriebszeiten durch den Einsatz von Videotechnik
e. Mehrfache unregelmäßige Bestreifung und Kontrolle der Liegenschaften und Gebäude außerhalb der Betriebszeiten durch einen privaten Sicherheitsdienst
f. Einteilung der Unternehmensgebäude in unterschiedliche Sicherheitsbereiche (z.B. Verwaltung, Entwicklung usw.)
g. Ausstattung der Maßnahmen zur Objektsicherung (Einsatz eines privaten Sicherheitsdienstes, Einsatz von Videotechnik, Stahltüren, Umzäunung des Geländes, elektr. Rolltor)

02. Zugangskontrolle

Die Schlüssel zu den Räumlichkeiten, in denen die Auftragsdaten verarbeitet bzw. vernichtet werden, befinden sich in der ausschließlichen Obhut der Geschäftsleitung des Auftragnehmers sowie der zuständigen Mitarbeiter. Dritte haben zu den Räumlichkeiten keinen Zutritt. Die Vergabe von Schlüsseln ist schriftlich geregelt. Firmenfremde werden zentral in Empfang genommen und im Gebäude begleitet.

Eine Übersicht der Maßnahmen zur Zugangskontrolle:

a. Festlegung befugter Personen
b. Vorhandensein von Regelungen für Firmenfremde
c. Durchführung von Anwesenheitsaufzeichnungen
d. Vorhandensein von Passwörtern (bei PC-Arbeitsplätzen)
e. Anforderung der regelmäßigen Passwortänderung (bei PC-Arbeitsplätzen)

03. Zugriffskontrolle

Der Zugriff auf Systeme ist mit Benutzerkennungen und regelmäßig zu ändernden Passwörtern geschützt. Zugriffe von außen erfolgen durch ausgewählte Mitarbeiter mit Identifizierung gegenüber dem Datenverarbeitungssystem durch Identifikation und Authentifizierung. Aktuelle Virenscanner sind installiert. Es wird gewährleistet, dass zur Verarbeitung bestimmte Daten während ihres Transports gegen unberechtigte Einsichtnahme und Verlust geschützt sind (SSL, Verschlüsselung bei Datenfernübertragung):

a. Umsetzung von Teilzugriffsmöglichkeit auf Datenbestände und Funktionen
b. Durchführung einer Identifizierung gegenüber dem Datenverarbeitungssystem durch Identifikation und Authentifizierung
c. Überprüfung der Berechtigung, maschinell
d. Umsetzung von Regelungen zur Zugriffs- und Benutzerberechtigung
e. Durchführung der Auswertung von Protokollen

04. Trennungsgebot

Die Trennung der Datensätze erfolgt durch die physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern.

Es existieren folgende Maßnahmen zum Trennungsgebot:

a. Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
b. Logische Mandantentrennung (softwareseitig)

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) ...
  ... ist die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen. Unter Berücksichtigung und Wahrung der durch die jeweiligen Auftraggeber benannten Zwecke der Datenverarbeitung, findet eine Pseudonymisierung der personenbezogenen Daten, die im Zuge der sich aus dem Hauptvertrag zu erbringenden Leistungen ergeben, nicht statt. Bei Verarbeitungen der personenbezogenen Daten, die über den durch den Kunden im Voraus definierten Zweck hinausgehen, nämlich konkret der Verarbeitung der Daten zu statistischen Zwecken, findet zuvor eine Anonymisierung statt. Hierbei werden nicht personenbezogenen Extrakte einzelner Datensätze aus den Datenbanken entnommen und miteinander vermischt, so dass ein späterer Personenbezug nicht mehr ableitbar ist.

II. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

01. Weitergabekontrolle

Für die datenschutzgerechte Vernichtung von Fehldrucken und sonstigem Datenabfall stehen für kleine Mengen elektrische Einzelschredder sowie für größere Mengen ein Papiervernichtungscontainer eines gewerblichen Vernichters zur Verfügung.

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

a. Vorhandensein von Dokumentationen der Abruf- und Übermittlungsprogramme
b. Vorhandensein von Dokumentationen zu den Stellen, an die eine Übermittlung vorgesehen ist sowie deren Übermittlungswege
c. Durchführung einer Verschlüsselung (SSL, SFTP, SSH)
d. Feststellung zur Übermittlung befugter Personen
e. Lagerung von Datenträgern in Sicherheitsbereichen (Vorhandensein von Dateiarchiven bzw. Tresoren)
f. Durchführung regelmäßiger Bestandskontrollen (Tages-, Wochen-, Monatscheck)
g. Kontrollierte Vernichtung von Datenträgern (Papier und elektronische Datenträger) nach DIN 66399
h. Zertifiziertes Dokumentenvernichtungssystem

02. Eingabekontrolle

Um Eingaben, Änderungen und Löschungen nachvollziehen zu können, wird eine Historie der Änderungen erstellt, die die Änderung sowie den Benutzer enthält, der die Änderung vorgenommen hat. Die Rechte der Benutzer sind an die jeweiligen Arbeitsabläufe und Abteilungen angepasst.

Es existieren folgende Maßnahmen zur Eingabekontrolle:

a. Protokollierung der Eingabe, Änderung und Löschung von Daten
b. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
c. Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

01. Verfügbarkeitskontrolle

Um die Verfügbarkeit der Daten zu gewährleisten, werden regelmäßige Backups im Rechenzentrum erstellt (siehe TOM Rechenzentrum).

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

a. Vorhandensein und Umsetzung eines Konzeptes zur Durchführung von regelmäßigen Datensicherungen (Datensicherheitskonzept gem. IT-Grundschutz)
b. Überwachung der Betriebsparameter von Rechenzentren (SNMP, Nagios)

02. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Sollte das Problem einer korrupten Datenbank hervortreten, so sind geeignete Maßnahmen einer raschen Wiederherstellbarkeit getroffen worden, indem die korrupte Datenbank mithilfe eines RAID-10-Systems wiederhergestellt werden kann. Soweit auch dieser automatische Prozess erfolglos bleiben sollte, ist eine manuelle Erstellung von Backups innerhalb einer Stunde möglich.

Der Serverstandort beherbergt weiterhin geeignete Maßnahmen im Falle eines entzündenden Feuers, indem Feuerabsenkungsanlagen installiert worden sind.

Der Serverstandort ist außerdem so ausgestattet, dass er sich für einen Zeitraum von vier Tagen mit einem eigenem Notstromsystem versorgen kann, um so die Funktionalität der Server zu gewährleisten.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

01. Datenschutz-Management

02. Incident-Response-Management

- Identifizierung zur Zugangsfreischaltung durch die Zusammenführung eines nach SHA1-Standard gehashten Passwortes mit einem Salt-Hash generierten Passwortes
- Sperreinrichtung des Zuganges bei mehrmaligen Fehleingaben
- IP-Sperren bei Botangriffen
- IP-Blacklist (Drittländer, in die keine Kundenbeziehungen unterhalten werden, werden ausgeschlossen)
- Passwortaufforderung nach 30 Tagen (Passwort muss nach 30 Tagen geändert werden und bereits in der Vergangenheit generierte Passwörter können nicht mehr genutzt werden)
- Nutzername darf sich nicht in dem Passwort wiederfinden
- Vorgabe von Sonderzeichen, Groß- und Kleinschreibung innerhalb der Erstellung von Passwörtern
- Erstmalige von dem Auftragnehmer an den Auftraggeber gegebene Passwörter müssen unmittelbar mit der ersten Nutzung des Zuganges geändert werden
- Neu erstellte Passworte werden an die im Portal hinterleget E-Mail-Adresse gesendet
- Supportanfragen, die ggf. eine Auskunft von personenbezogenen Daten mit sich ziehen, werden nur nach Nennung eines im Voraus vergebenen PINS beantwortet
- Installierte physische und softwaretechnischen Firewalls

03. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

- Privatschalter (Sofern gebucht, werden bei Betätigung des Privatschalters die GPS-Ortungsdaten nicht mehr aufgezeichnet.)
- Privattaste Smartphone (Start- und Endpunkt der zurückgelegten Strecke bei dem Produkt Logbook, können im Nachhinein mithilfe der Privattaste der Smartphone-App als Privatfahrt deklariert werden. Hierbei werden die aufgezeichneten Punkte unmittelbar unwiderruflich gelöscht)
- Optionale Möglichkeit der Nutzung von Zeitfiltern, um das Life-Tracking von Personen verhindern zu können
- Portfreigabe-, Portgruppenmanagement

04. Auftragskontrolle

Alle Mitarbeiter des Auftragnehmers sind vertraglich zur Vertraulichkeit verpflichtet worden und werden fortlaufend auf den Bereich Datenschutz sensibilisiert.