

Anlage 2: Technische und organisatorische Maßnahmen (TOM)

Gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. G) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. D)

Unternehmen:

belboon GmbH
Weinmeisterstraße 12-14
10178 Berlin

1. Psydonymisierung / Anonymisierung

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;

1.1. IP-Adressen

- Anonymsierung der IP-Adressen, vor der Verarbeitung und Speicherung werden die IP-Adressen vom Typ IPv4 um das letzte Oktett und die IPv6-Adressen um die letzten 80 Bits anonymisiert. Erst danach erfolgt die Verarbeitung der Events. Durch diese Anonymisierung sind die IP-Adressen kein personenbezogenes Datum mehr.
- Zusätzlich für das neue belboon System schauen Sie bitte in Anhang 1, in die TOM's unseres technischen Dienstleisters Ingenious Technologies.

2. Verschlüsselung

2.1. HTTPS-Verschlüsselung

- Verschlüsselung der belboon Website & Kundenbereich, hierbei wird automatisch über HTTPS verschlüsselt.
- Beim Conversion Code des Advertisers kann optional auch HTTPS verwendet werden.
- Auch Publisher können optional einen HTTPS Werbemittelcode einbinden.

- Findet die Kommunikation über HTTPS statt, so erfolgt die Übermittlung der Daten mit einer SSL-Verschlüsselung (SHA256).
- Zusätzlich für das neue belboon System schauen Sie bitte in Anhang 1, in die TOM's unseres technischen Dienstleisters Ingenious Technologies.

2.2. Passwort – Verschlüsselung (Kunden Plattform)

- Alle Passwörter der Kundenplattform werden unter Hinzunahme eines sog. „Salts“ in gehashter Form gespeichert.
- Zusätzlich für das neue belboon System schauen Sie bitte in Anhang 1, in die TOM's unseres technischen Dienstleisters Ingenious Technologies.

2.3. Festplatten Verschlüsselung (Notebooks)

- Alle Festplatten der Mitarbeiter Notebooks sind mit einem HDD-Kennwort, welches sich auf der Festplatte selbst befindet, geschützt.

3. Vertraulichkeit

3.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

- Manuelles Schließsystem
 - Klingelanlage mit Kamera & Gegensprechanlage
 - Schlüsselliste
 - Transponder
 - Sorgfalt bei der Auswahl des Reinigungsdienstes
-
- Zusätzlich für das neue belboon System schauen Sie bitte in Anhang 1, in die TOM's unseres technischen Dienstleisters Ingenious Technologies.

3.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

- Login mit Benutzername und Passwort
 - ESET Protect Cloud Vers. 3.4.11.1 Firewall
 - VPN bei Remote Zugriff auf Finanzsysteme (LANCOM VPN 3.02)
 - Verschlüsselung von Notebooks
 - Verwalten von Benutzerberechtigungen
 - BIOS Schutz (separates Passwort), zum Schutz vor Änderungen an der Konfiguration des jeweiligen Gerätes
 - Zentrale Passwortvergabe
 - Erstellen von Benutzerprofilen
 - Allg. Datenschutz Richtlinien und Hinweise
 - Information manuelle Desktopsperre
-
- Zusätzlich für das neue belboon System schauen Sie bitte in Anhang 1, in die TOM's unseres technischen Dienstleisters Ingenious Technologies.

3.3. 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. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

- Einsatz eines Berechtigungskonzeptes
- Aktenschredder
- Minimale Anzahl an Administratoren

- Verwaltung Benutzerrechte durch Administratoren
- Zusätzlich für das neue belboon System schauen Sie bitte in Anhang 1, in die TOM's unseres technischen Dienstleisters Ingenious Technologies.

3.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

- Trennung von Produktiv und Testumgebung
- Physikalische Trennung von (Systeme / Datenbank / Datenträger)
- Mandantenfähigkeit relevanter Anwendungen
- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten
- Zusätzlich für das neue belboon System schauen Sie bitte in Anhang 1, in die TOM's unseres technischen Dienstleisters Ingenious Technologies.

4. Integrität

4.1. Weitergabeprotokolle

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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

- Einsatz VPN
- Bereitstellung über verschlüsselte Verbindungen (https, SSH)
- Zusätzlich für das neue belboon System schauen Sie bitte in Anhang 1, in die TOM's unseres technischen Dienstleisters Ingenious Technologies.

4.2. Eingabeprotokolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten im Rechenzentrum
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzer (nicht Benutzergruppen) im Rechenzentrum
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

5. Verfügbarkeit, Belastbarkeit und Wiederherstellung

5.1. Verfügbarkeitsprotokolle

Maßnahmen, die geeignet sind, Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, RAID-Systeme, Plattenspiegelungen etc.

- Feuerlöscher Büro
 - Feuer- und Rauchmeldeanlage im Rechenzentrum
 - Fremdüberwachung Temperatur und Feuchtigkeit
 - USV
 - Kontrolle Sicherungsvorgang (stichprobenhaft)
 - Aufbewahrung Backups
-
- Zusätzlich für das neue belboon System schauen Sie bitte in Anhang 1, in die TOM's unseres technischen Dienstleisters Ingenious Technologies.

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technisch organisatorischen Maßnahmen

6.1. Datenschutzmanagement

- Externer Datenschutzbeauftragter
- Regelmäßige Sensibilisierung der Mitarbeiter (mindestens jährlich)
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
- Zentrale Dokumentation aller Verfahrenshinweise
- Überprüfung der TOM's mindestens einmal jährlich

6.2. Incident-Response-Management

- Firewall
- Einsatz von SPAM Filtern
- Schutz der Website DDOS-Schutz (Cloudflare)
- Einsatz von Virenscannern

- Zusätzlich für das neue belboon System schauen Sie bitte in Anhang 1, in die TOM's unseres technischen Dienstleisters Ingenious Technologies.

6.3. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Vorauswahl von Standardanbietern
- Auswahl des Auftragnehmers und Sorgfaltspflichten (gerade in Bezug auf Datenschutz, DSGVO Konformität und Datensicherheit)
- Unterjährige Stichproben zur Sicherstellung des Datenschutzes

Anhang 1

Technische und organisatorische Maßnahmen unseres Plattform Dienstleisters,

Ingenious Technologies AG
Französische Straße 48
10117 Berlin
Deutschland

gemäß § 64 Abs. 3 BDSG-neu.

Der Auftragnehmer (AN) sichert dem Auftraggeber (AG) zu, folgende technische und organisatorische Maßnahmen gemäß § 64 Abs. 3 BDSG-neu und der dazugehörigen Anlage getroffen zu haben:

1. Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.

Die Applikationsserver des AN werden ausschließlich in den Rechenzentren der jeweiligen Cloud Services Provider in dem Gebiet der Europäischen Union gehostet, so findet die Datenspeicherung und Datenverarbeitung von Personenbezogenen Daten ausschließlich in dem EU-Gebiet statt. Der physische Zugang zu den Einrichtungen, mit denen personenbezogene Daten verarbeitet wird, ist durch den jeweiligen Cloud Services Provider ausschließlich auf benannte autorisierte Personen beschränkt, so dass der Zutritt zu IT-Systemen und Datenverarbeitungsanlagen für unbefugten Personen verwehrt wird.

In der Cloud verwendet der AN sowohl Plattform as a Service Dienste (PaaS) als auch Infrastructure as a Service Dienste (IaaS).

Für die Plattform as a Service (PaaS) Dienste:

Cloud Provider führt regelmäßige Systemupdates und Patches auf den unterliegenden physischen und virtuellen Maschinen durch.

Für die Infrastructure as a Service (IaaS):

Der AN führt regelmäßige OS-Aktualisierungen und Sicherheitsupdates auf allen virtuellen Maschinen des Cloud IaaS durch.

Beschreibung des Zugangskontrollsystems:

- | | |
|---|--|
| <input checked="" type="checkbox"/> Alarmanlage | <input checked="" type="checkbox"/> Absicherung von Gebäudeschächten |
| <input checked="" type="checkbox"/> Automatisches Zugangskontrollsystem | <input checked="" type="checkbox"/> Chipkarten-/Transponder-Schließsystem |
| <input checked="" type="checkbox"/> Schließsystem mit Codesperre | <input checked="" type="checkbox"/> Manuelles Schließsystem |
| <input type="checkbox"/> Biometrische Zugangssperren | <input checked="" type="checkbox"/> Videoüberwachung der Zugänge |
| <input checked="" type="checkbox"/> Lichtschranken / Bewegungsmelder | <input checked="" type="checkbox"/> Sicherheitsschlösser |
| <input checked="" type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input checked="" type="checkbox"/> Personenkontrolle beim Pförtner / Empfang |
| <input checked="" type="checkbox"/> Protokollierung der Besucher | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input checked="" type="checkbox"/> Sorgfältige Auswahl von Wachpersonal | <input checked="" type="checkbox"/> Tragepflicht von Berechtigungsausweisen |

2. Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderens oder Löschens von Datenträgern.

Die Daten werden auf logischen Datenträgern gespeichert, der physische Transport der Datenträger findet nicht statt, da die Anwendungs-Infrastruktur vollständig beim Cloud Services Provider betrieben wird. Für die Verbindung vom Office zum Rechenzentrum wird eine VPN-Verbindung verwendet (Verschlüsselung: AES 256). Die Übermittlung der personenbezogenen Daten zwischen dem Backend und dem Anwender-UI erfolgt mit einer SSL-Verschlüsselung (minimale erlaubte Verschlüsselung: TLS 1.0). Die Speicherung von nichtverschlüsselten Personenbezogenen Daten in getrennten Applikationsmodulen erfolgt in einer pseudonymisierten Form, so dass die Zuordnung der Daten zu Personen nur über die Referenz-IDs erfolgen kann. Die AN IT-Administratoren haben keinen Zugriff auf gespeicherte

personenbezogene Daten, da die einzelnen Datensätze durch die Applikationslogik verschlüsselt und nur durch die Applikationslogik wieder entschlüsselt werden können.

Beschreibung der Datenträgerkontrollsystems:

- | | |
|---|---|
| <input checked="" type="checkbox"/> Verwaltung der Rechte durch Systemadministrator | <input checked="" type="checkbox"/> Weitergabe von Daten in anonymisierter oder pseudonymisierter Form |
| <input checked="" type="checkbox"/> Anzahl der Administratoren auf das „Notwendigste“ reduziert | <input type="checkbox"/> Beim physischen Transport: sichere Transportbehälter/-verpackungen |
| <input checked="" type="checkbox"/> Erstellen eines Berechtigungskonzepts | <input type="checkbox"/> Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen |
| <input checked="" type="checkbox"/> Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel | <input checked="" type="checkbox"/> Verschlüsselung/Passwortschutz von Datenträgern in Laptops / Notebooks |
| <input checked="" type="checkbox"/> Verschlüsselung von Datenträgern | <input checked="" type="checkbox"/> Sichere Aufbewahrung von Datenträgern |
| <input checked="" type="checkbox"/> physische Löschung von Datenträgern vor Wiederverwendung | <input checked="" type="checkbox"/> ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) |
| <input type="checkbox"/> Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) | <input type="checkbox"/> Protokollierung der Vernichtung |

3. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

Die Erteilung und Änderung der Zugriffsrechte für die AN-Anwendungsadministratoren erfolgt durch die Rollen- und Rechteverwaltung in der Anwendung. Die AN IT-Administratoren haben keinen Zugriff auf gespeicherte personenbezogene Daten, da die einzelnen Datensätze durch die Applikationslogik verschlüsselt und nur durch die Applikationslogik wieder entschlüsselt werden können. Die physikalische Speicherung der Daten erfolgt in der Cloud auf die logische Storage-Einheiten, so dass die Daten

dabei fragmentiert und auf mehrere physikalische Laufwerke aufgeteilt werden. Die Daten-Fragmente werden beim Lesen durch die Software-Layer erneut zusammengesetzt.

Beschreibung des Speicherkontrollsystems:

- | | |
|--|--|
| <input checked="" type="checkbox"/> Fragmentierung der Daten bei Speicherung | <input checked="" type="checkbox"/> Verschlüsselung von Datenträgern |
| <input checked="" type="checkbox"/> Authentifikation mit Benutzername / Passwort | <input checked="" type="checkbox"/> Verschlüsselung/Passwortschutz von Datenträgern in Laptops / Notebooks |
| <input type="checkbox"/> Authentifikation mit biometrischen Verfahren | <input checked="" type="checkbox"/> Zuordnung von Benutzerprofilen zu Mandanten |

4. Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

Die AN IT-Infrastruktur befindet sich vollständig in der Cloud. Die IT-Administratoren haben Zugang ausschließlich über persönliche asymmetrische RSA-Keys (2048 Bit), die Keys sind zusätzlich mit individuellen Passwörtern geschützt. Die Anmeldungen der IT-Administratoren auf den Servern werden protokolliert. Jede Erteilung bzw. Änderung der Zugriffsrechte erfolgt nach Vier-Augen-Prinzip und wird protokolliert. Die Erforderlichkeit der Zugriffsrechte der Nutzer wird regelmäßig, alle 90 Tage überprüft. Der Offboarding-Prozess stellt sicher, dass Nutzerzugänge im Falle eines Ausscheidens rechtzeitig widerrufen werden. Die Benutzerkennungen sind eindeutig und individuell. Die Passwörter sind min. 8 Zeichen lang und müssen Ziffern, Sonderzeichen sowie kleine und große Buchstaben enthalten. Die Passwörter müssen nach 90 Tagen geändert werden. In der Passwort-Historie werden die 6 letzten Passwörter gespeichert. Nach 3-facher Fehleingabe erfolgt eine automatische Account-Sperrung.

Beschreibung des Benutzerkontrollsystems:

- | | |
|---|---|
| <input checked="" type="checkbox"/> Zuordnung von Benutzerprofilen zu IT-Systemen | <input checked="" type="checkbox"/> Verwaltung der Rechte durch Systemadministrator |
|---|---|

- | | |
|--|---|
| <input checked="" type="checkbox"/> Authentifikation mit Benutzername / Passwort | <input type="checkbox"/> Authentifikation mit biometrischen Verfahren |
| <input checked="" type="checkbox"/> Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel | <input checked="" type="checkbox"/> Einsatz von VPN-Technologie |
| <input checked="" type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | <input checked="" type="checkbox"/> Einsatz von Anti-Viren-Software |

5. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Die Überwachung des Berechtigungskonzeptes auf der Applikationsebene obliegt dem AG. Das dafür notwendige UI zum Verwalten der Rollen und der Zugriffsrechte wird vom AN zur Verfügung gestellt. Die Änderungen werden protokolliert. Die Erteilung und Änderung der Zugriffsrechte für die AN-Anwendungsadministratoren erfolgt durch dieselbe Rollen- und Rechteverwaltung in der Anwendung.

Beschreibung des Zugriffskontrollsystems:

- | | |
|--|---|
| <input checked="" type="checkbox"/> Erstellen eines Berechtigungskonzeptes | <input checked="" type="checkbox"/> Verwaltung der Rechte durch Anwendungs-Administratoren |
| <input checked="" type="checkbox"/> Anzahl der Administratoren auf das „Notwendigste“ reduziert | <input checked="" type="checkbox"/> Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel |
| <input checked="" type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | <input checked="" type="checkbox"/> Mandantentrennung |

6. Übertragungskontrolle

Gewährleistung, 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.

Es werden keine Daten weitergegeben, da die Infrastruktur vollständig beim Cloud Provider betrieben wird. Für die Verbindung vom Office zum Rechenzentrum wird eine VPN-Verbindung verwendet (Verschlüsselung: AES 256). Die Übermittlung der personenbezogenen Daten zwischen dem Backend und dem Anwender-UI erfolgt mit einer SSL-Verschlüsselung (minimale erlaubte Verschlüsselung: TLS 1.0). Die Speicherung von nichtverschlüsselten Personenbezogenen Daten in getrennten Applikationsmodulen erfolgt in einer pseudonymisierten Form, so dass die Zuordnung der Daten zu Personen nur über die Referenz-IDs erfolgen kann.

Beschreibung der Weitergabekontrolle:

- | | |
|---|--|
| <input checked="" type="checkbox"/> Einrichtungen von Standleitungen bzw. VPN-Tunneln | <input checked="" type="checkbox"/> Weitergabe von Daten in anonymisierter oder pseudonymisierter Form |
| <input type="checkbox"/> E-Mail-Verschlüsselung | <input type="checkbox"/> Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen |
| <input type="checkbox"/> Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen | |

7. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

Die Änderungen werden in derselben Datenbank protokolliert, in der auch die zu ändernden Daten gespeichert werden. So gelten für die Protokollierungsdaten die gleichen Regeln wie für die Daten selbst. Die Log-Dateien der Applikationsserver verlassen das geschützte Netzwerk nicht und werden nach 30 Tagen gelöscht. Nur die AN IT-Administratoren haben Zugriff auf das geschützte Netzwerk. Der Zugriff erfolgt über den asymmetrischen RSA-Verfahren mit der 2048-Bit Key-Länge (individuelle Keys).

Beschreibung des Eingabekontrollsystems:

- | | |
|---|--|
| <input checked="" type="checkbox"/> Protokollierung der Eingabe, Änderung und Löschung von Daten | <input type="checkbox"/> Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. |
| <input checked="" type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) | <input type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |
| <input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts | |

8. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

Es werden keine Daten sowie Datenträger transportiert, da die Infrastruktur vollständig beim Cloud Services Provider betrieben wird. Für die Verbindung vom Office zum Rechenzentrum wird eine VPN-Verbindung verwendet (Verschlüsselung: AES 256). Die Übermittlung der personenbezogenen Daten zwischen dem Backend und dem Anwender-UI erfolgt mit einer SSL-Verschlüsselung (minimale erlaubte Verschlüsselung: TLS 1.0). Die Speicherung von nichtverschlüsselten Personenbezogenen Daten in getrennten Applikationsmodulen erfolgt in einer pseudonymisierten Form, so dass die Zuordnung der Daten zu Personen nur über die Referenz-IDs erfolgen kann.

Beschreibung der Transportkontrollsystems:

- | | |
|---|--|
| <input checked="" type="checkbox"/> Einrichtungen von Standleitungen bzw. VPN-Tunneln | <input checked="" type="checkbox"/> Weitergabe von Daten in anonymisierter oder pseudonymisierter Form |
| <input type="checkbox"/> E-Mail-Verschlüsselung | <input type="checkbox"/> Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen |

- | | |
|---|---|
| <input type="checkbox"/> Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen | <input type="checkbox"/> Beim physischen Transport: sichere Transportbehälter/-verpackungen |
|---|---|

9. Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können.

Es werden regelmäßig Backups der Daten erstellt. Die Backups werden in demselben geschützten Netzwerk aufbewahrt, in dem auch die Daten verarbeitet werden. Die physikalische Speicherung der Backups erfolgt in der Cloud Umgebung auf den dedizierten logischen Storage-Einheiten.

Beschreibung des Wiederherstellbarkeitssystems:

- | | |
|--|--|
| <input checked="" type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV) | <input checked="" type="checkbox"/> Klimaanlage in Serverräumen |
| <input checked="" type="checkbox"/> Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | <input checked="" type="checkbox"/> Schutzsteckdosenleisten in Serverräumen |
| <input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen | <input type="checkbox"/> Feuerlöschgeräte in Serverräumen |
| <input checked="" type="checkbox"/> Alarmmeldung bei unberechtigten Zutritten zu Serverräumen | <input checked="" type="checkbox"/> Erstellen eines Backup- & Recoverykonzepts |
| <input checked="" type="checkbox"/> Testen von Datenwiederherstellung | <input checked="" type="checkbox"/> Erstellen eines Notfallplans |
| <input checked="" type="checkbox"/> Aufbewahrung von Datensicherung in separaten logischen Storage-Einheiten | <input checked="" type="checkbox"/> Serverräume nicht unter sanitären Anlagen |

10. Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Die IT-Infrastruktur und die Funktionsfähigkeit der Anwendung wird permanent auf mehreren Ebenen

überwacht. Bei Störungen werden qualifizierte Mitarbeiter alarmiert. Die Behebung der Störungen erfolgt nach dem Notfallplan.

Beschreibung des Zuverlässigkeitssystems:

- | | |
|---|--|
| <input checked="" type="checkbox"/> Monitoring der IT-Infrastruktur und der Anwendung auf mehreren Ebenen | <input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen |
| <input checked="" type="checkbox"/> Alarmierung durch Emails und SMS | <input checked="" type="checkbox"/> Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen |
| <input checked="" type="checkbox"/> Erstellen eines Notfallplans | <input checked="" type="checkbox"/> Serverräume nicht unter sanitären Anlagen |

11. Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

In der Applikationslogik werden umfangreiche Regeln zum Prüfen und Sicherstellen der Datenintegrität implementiert. In der Datenbank wird Datenintegrität u.A. durch Normalisierungskonzepte und Constraints sichergestellt.

Beschreibung des Datenintegritätssystems:

- | | |
|--|---|
| <input checked="" type="checkbox"/> Regeln zum Verifizieren der Daten bei der Eingabe und Änderungen | <input checked="" type="checkbox"/> Constraints auf Datenbankobjekten |
| <input checked="" type="checkbox"/> Daten-Normalisierung | |

12. Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Die Auswahl der Unterauftragnehmer erfolgt unter größter Sorgfalt, die Verarbeitung der Daten erfolgt auf Basis des AV-Vertrages gemäß Art. 28 Datenschutz-Grundverordnung.

Beschreibung des Auftragskontrollsystems:

- | | |
|---|---|
| <input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) | <input checked="" type="checkbox"/> vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen |
| <input checked="" type="checkbox"/> schriftliche Weisungen an den Auftragnehmer (z.B. durch Datenverarbeitungsvertrag) | <input checked="" type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis |
| <input checked="" type="checkbox"/> Auftragnehmer hat Datenschutzbeauftragten bestellt | <input checked="" type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |
| <input checked="" type="checkbox"/> Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart | <input checked="" type="checkbox"/> laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten |

13. Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Die Backups werden in demselben geschützten Netzwerk aufbewahrt, in dem auch die Daten verarbeitet werden. Keine Datenträger verlassen das geschützte Netzwerk. Die physikalische Speicherung der Daten erfolgt in der Cloud auf die logische Storage-Einheiten, so dass die Daten dabei fragmentiert und auf mehrere physikalischen Laufwerke aufgeteilt werden. Die Daten-Fragmente werden beim Lesen durch die Software-Layer erneut zusammengesetzt. Nur die AN IT-Administratoren haben Zugriff auf das Netzwerk. Der Zugriff erfolgt über den asymmetrischen RSA-Verfahren mit der 2048-Bit Key-Länge (individuelle Keys).

Beschreibung des Verfügbarkeitskontrollsystems:

- | | |
|---|---|
| <input checked="" type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV) | <input checked="" type="checkbox"/> Klimaanlage in Serverräumen |
|---|---|

- | | |
|--|--|
| <input checked="" type="checkbox"/> Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | <input checked="" type="checkbox"/> Schutzsteckdosenleisten in Serverräumen |
| <input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen | <input type="checkbox"/> Feuerlöschgeräte in Serverräumen |
| <input checked="" type="checkbox"/> Alarmmeldung bei unberechtigten Zutritten zu Serverräumen | <input checked="" type="checkbox"/> Erstellen eines Backup- & Recoverykonzepts |
| <input checked="" type="checkbox"/> Testen von Datenwiederherstellung | <input checked="" type="checkbox"/> Erstellen eines Notfallplans |
| <input checked="" type="checkbox"/> Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort | <input checked="" type="checkbox"/> Serverräume nicht unter sanitären Anlagen |

14. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Bei der Speicherung der Kundendaten besteht eine logische, bei der Verarbeitung die physikalische Mandantentrennung. Produktiv- und Testsysteme sind voneinander physikalisch getrennt. Die Speicherung von nichtverschlüsselten Personenbezogenen Daten in getrennten Applikationsmodulen erfolgt in einer pseudonymisierten Form, so dass die Zuordnung der Daten zu Personen nur über die Referenz-IDs erfolgen kann.

Beschreibung des Trennbarkaietssystems:

- | | |
|--|---|
| <input type="checkbox"/> physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern | <input checked="" type="checkbox"/> Logische Mandantentrennung (softwareseitig) |
| <input checked="" type="checkbox"/> Erstellung eines Berechtigungskonzepts | <input type="checkbox"/> Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden |
| <input type="checkbox"/> Versehen der Datensätze mit Zweckattributen/Datenfeldern | <input type="checkbox"/> Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System |
| <input checked="" type="checkbox"/> Festlegung von Datenbankrechten | <input checked="" type="checkbox"/> Trennung von Produktiv- und Testsystem |