Technische und organisatorische Maßnahmen zur Datensicherheit

Art. 5 Abs. 1 f, Art. 32 DS-GVO (Art. 24, 25, 36 DS-GVO)

Die SitePlan GmbH sichert zu, folgende technische und organisatorische Maßnahmen zur Datensicherheit (konform zur DS-GVO) getroffen zu haben:

1. Vertraulichkeit

Absicherung, dass Daten nur befugten Personen zugänglich zu machen sind; bedroht sind dabei nicht nur die Daten an sich, sondern auch die Systeme und Konfigurationen. Es müssen Sicherheitsmaßnahmen erhoben werden, damit ein unbefugter Zugriff auf gespeicherte und übermittelte Daten verhindert werden kann.

1.1. Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie vertraulichen Akten und Datenträgern physisch verwehren.

Unser Anwendungsfall:

Die Verarbeitung von Daten, die bei der Verwendung der SitePlan-App anfallen, erfolgt ausschließlich durch Mitarbeiter und Systeme der SitePlan GmbH. Die Systeme laufen auf gemieteten Server-Instanzen eines großen, international renommierten Cloud-Anbieters. Dieser gewährleistet neben der DS-GVO konformen Speicherung der Daten auch die physische und digitale Sicherheit durch eine große Anzahl an IT-Sicherheitsexperten. Der Standort des Datenzentrums ist Dublin (Irland), wodurch gewährleistet ist, dass die Daten innerhalb der EU-Zone gespeichert werden. Für Entwicklungs-, Test- und Wartungszwecke haben die IT-Arbeitsgeräte der Mitarbeiter der SitePlan GmbH Zugriff auf die Server-Instanzen.

Unsere Maßnahmen:

- gewährleistet durch unseren Cloud-Partner
    - physische Sicherheit des Datenzentrums
- gewährleistet durch unseren Büro-Vermieter
    - Zugang zum Büro 24/7 nur mit Chip-Schlüssel
    - Protokollierte Ausgabe der Chip-Schlüssel
    - Videoüberwachung im Eingangsbereich
    - Nächtliche Überwachung durch Sicherheitspersonal, sowie Alarmanlage

1.2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

Unser Anwendungsfall:

Die Maßnahmen der Zugangskontrolle umfassen einerseits digitale Sicherheitsmaßnahmen des Servers bzw. Backends, um einen externen Zugriff durch Dritte zu unterbinden. Andererseits umfassen diese auch physische Maßnahmen zur Sicherung der IT-Arbeitsgeräte über die ein Server-Zugang möglich ist.

Unsere Maßnahmen:

- IT-Arbeitsgeräte
  - Passwortgeschützter Zugang zu IT-Arbeitsgeräten (Laptops)
  - Automatische Sperrung von Laptops bei Inaktivität
  - Laptops werden über Nacht nicht im Büro gelagert
- Server / Backend
  - personifizierter & bestätigter Account pro User (E-Mail-Adresse)
  - Authentifizierung durch OAuth und API-Zugriff via JWT
  - Verschlüsselung der gesamten Kommunikation über HTTPS/TLS1.2
  - Verschlüsselte Speicherung der Passwörter in Datenbank (One-Way mit Salt)
  - Hochgeladene Dateien (z.B. Pläne und Fotos) werden mit AES-256 verschlüsselt abgespeichert, sind vor externem Zugriff geschützt (nicht über öffentliche URL abrufbar) und werden zur Verarbeitung ausschließlich mit HTTPS/TLS1.2 verschlüsselt übertragen

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Unser Anwendungsfall:

Die Zugriffskontrolle auf Daten wird über ein Permission-Modell auf Rollenebene abgewickelt und regelmäßig auf Zuverlässigkeit getestet.

Unsere Maßnahmen:

- Benutzerverwaltung und Berechtigungskonzept auf Rollenebene (Member, Admin, Owner)
- Regelmäßige Tests der Zugriffsrechte durch Benutzer und Rollen

1.4. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Unsere Maßnahmen:

- Berechtigungskonzept auf Rollenebene (Member, Admin, Owner)
- Datenspeicherung auf Mandantenbasis (je ein Mandant pro Kunde)
- Trennung von Test- und Produktivsystemen

1.5. Pseudonymisierung

Maßnahmen, die gewährleisten, dass personenbezogene Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, indem diese zusätzlichen Informationen gesondert aufbewahrt werden.

Unser Anwendungsfall:

Aktuell liegt bei SitePlan kein Anwendungsfall vor, bei dem Maßnahmen zur Pseudonymisierung angewendet werden müssen. Sollte in Zukunft ein Anwendungsfall auftreten, werden Maßnahmen ergriffen, dass diese Daten keiner spezifischen Person zugeordnet werden können.

Unsere Maßnahmen:

- keine

2. Integrität

Daten und Systeme müssen korrekt, unverändert und verlässlich sein. Bei einem Angriff auf die Integrität käme es beispielsweise zur Verfälschung der Daten, oder einer fehlerhaften Funktion der Hard- und/oder Software, sodass falsche Ergebnisse geliefert würden und die Hard- und Software unzuverlässig wäre. Der „Angriff“ kann daher auch versehentlich durch Bedienungsfehler erfolgen.

2.1. 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 sowie Maßnahmen mit denen überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist.

Unsere Maßnahmen:

- Verschlüsselung der gesamten Kommunikation zwischen Nutzer und Server über HTTPS/TLS1.2

- Aufbereitung von Datenbankabfragen im Server zur Vermeidung von DB-Injections

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Unsere Maßnahmen:

- Protokollierung der Server-Aktivitäten in Log-Files

2.3. Authentizität

Angegeben werden sollten hier alle Maßnahmen, die Echtheit, Zuverlässigkeit und Glaubwürdigkeit einer Mitteilung sicherstellen. Ein Angriff wäre die unbefugte Erzeugung von Nachrichten z.B. unter falscher Identität. Auch die Authentizität von IT-Systemen muss gewährleistet sein.

Unsere Maßnahmen:

- Verschlüsselung der gesamten Kommunikation zwischen Nutzer und Server über HTTPS/TLS1.2

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

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

Unser Anwendungsfall:

Für die Speicherung aller Daten, die bei der Verwendung der App durch die SitePlan GmbH verarbeitet werden, arbeiten wir mit einem großen, international renommierten Cloud-Anbieter zusammen. Dieser gewährleistet neben der DS-GVO konformen Speicherung der Daten auch die physische und digitale Sicherheit durch eine große Anzahl an IT-Sicherheitsexperten. Der Standort des Datenzentrums ist Dublin (Irland), wodurch gewährleistet ist, dass die Daten innerhalb der EU-Zone gespeichert werden.

Unsere Maßnahmen:

- gewährleistet durch unseren Cloud-Partner
    - Redundante Speicherung auf mehreren Instanzen in derselben Zone (=Standort)
    - beim Ausfall einer Instanz nahtloser Wechsel auf eine andere Instanz
    - dadurch gewährleistete Verfügbarkeit von 99,99%
    - täglicher Durchlauf des Datensicherungsverfahrens
- regelmäßige Tests der Datenwiederherstellung

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Daten und IT-Systeme stehen zur Verfügung und können von befugten Personen genutzt werden. Eine unbefugte Unterbrechung z.B. durch Serverausfall oder Ausfall von Kommunikationsmitteln stellt einen Angriff auf die Verfügbarkeit dar.

4.1. Auftragskontrolle

Maßnahmen, die gewährleisten, dass in einem Auftragsdatenverarbeitungsverhältnis jede Verarbeitung von personenbezogenen Daten nur im Rahmen der ergangenen Weisungen und Vorgaben des Auftraggebers erfolgt.

Unser Anwendungsfall:

Die Verarbeitung von personenbezogenen Daten erfolgt nur durch die SitePlan GmbH. Es gibt keine Drittunternehmen, die für die Verarbeitung von Auftragsdaten beauftragt wurden und es ist auch nicht geplant in der Zukunft Teile der Datenverarbeitung auszulagern.

Unsere Maßnahmen:

- keine

4.2. Datenschutzmanagement

Das Datenschutzmanagement beschreibt eine Methode, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, zu organisieren, zu steuern und zu kontrollieren.

Unsere Maßnahmen:

- Vertragliche Verpflichtung zur Wahrung des Datengeheimnisses aller Mitarbeiter der SitePlan GmbH
- Regelmäßige Datenschutzschulung aller Mitarbeiter der SitePlan GmbH
- Regelmäßige Prüfung der gesetzten technischen und organisatorischen Maßnahmen zur Datensicherheit
- Regelmäßige Beurteilung der Methoden des Datenschutzmanagements

4.3. Incident-Response-Management

Entwicklung und Darstellung des Prozesses im Fall erkannter oder vermuteter Sicherheitsvorfälle / Störungen im IT-Bereich.

Unsere Maßnahmen:

- Inkenntnissetzung der betroffenen Kunden/User

- sofortige temporäre Sperrung der betroffenen User
- Aufforderung zur Zurücksetzung der Passwörter der betroffenen User
- tiefgehende Analyse der potenziellen Schwachstelle
- Behebung aller sicherheitskritischer Lücken

4.4. Datenschutzfreundliche Voreinstellungen (Data protection by default)

Ein Produkt oder ein Dienst weist ohne weiteres Zutun beim ersten Einschalten bzw. Aufruf die datenschutzfreundlichsten Einstellungen und Komponenten auf. Beispiel: Verzicht auf vorangekreuzte Einwilligungserklärungen oder ähnliche vorausgewählte Einstellungen. Es soll nicht ausreichen, dass ein Nutzer Wahl- und Gestaltungsmöglichkeiten hat.

Unser Anwendungsfall:

Für die Registrierung zur SitePlan-App werden vom Nutzer lediglich die minimalst notwendigen Daten, wie Vorname, Nachname und E-Mail-Adresse abgefragt. Die Zustimmung zu Geschäftsbedingungen oder Einwilligungserklärungen muss vom Nutzer proaktiv erfolgen und ist nicht vorausgewählt. Für die Nutzung jeglicher Funktionen der SitePlan-App werden nur die wirklich für die Funktionsweise essentiellen Daten gefordert.

Unsere Maßnahmen:

- Regelmäßige Beurteilung der geforderten Nutzerdaten auf ihre Notwendigkeit

4.5. Datenschutz durch Technik (Data protection by design)

Technische und organisatorische Maßnahmen zur Datenvermeidung, z.B. Pseudonymisierung, Verschlüsselung und Zugangs- und Zutrittskontrollen, Anonymisierung – s.o.

Unser Anwendungsfall:

Für die Registrierung zur SitePlan-App werden vom Nutzer lediglich die minimalst notwendigen Daten, wie Vorname, Nachname und E-Mail-Adresse abgefragt. Für die Nutzung jeglicher Funktionen der SitePlan-App werden nur die wirklich für die Funktionsweise essentiellen Daten gefordert.

Unsere Maßnahmen:

- Regelmäßige Beurteilung der geforderten Nutzerdaten auf ihre Notwendigkeit