ANHANG - Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter gewährleistet, dass die folgenden technischen und organisatorischen Maßnahmen getroffen wurden:

1. Maßnahmen zur Gewährleistung der Vertraulichkeit

1.1. Physische Zugangskontrolle

Maßnahmen zur Vermeidung des physischen Zugangs unbefugter Personen zu IT- und Datenverarbeitungssystemen für die Verarbeitung personenbezogener Daten und zu vertraulichen Dateien und Speichermedien:

In Mailjet-Räumlichkeiten:

- Türsicherheit (elektronisches Ausweissystem mit kontrollierter Schlüsselzuordnung)
- Aufzugsicherheit (Aufzug-Zugangscodes)
- Überwachungseinrichtungen (Alarmsysteme und Videoüberwachung)
- Gesicherter IT-Raum
- Feueralarm und Feuerlöscher
- Kontrollsystem für Besucher

In Datenzentren:

- Umzäunung
- Türsicherheit (elektronisches Ausweissystem mit kontrollierter Schlüsselzuordnung)
- Überwachungseinrichtungen (Bewegungsmelder, Alarmsysteme, Videoüberwachung)
- Feueralarm und Feuerlöscher
- Kontrollsystem für Besucher
- Sicherheitspersonal vor Ort rund um die Uhr

1.2. Logische Zugangs- und Datenzugriffskontrolle

Maßnahmen zur Vermeidung der Verarbeitung oder Nutzung geschützter Daten durch unbefugte Personen, sodass die Daten während der Verarbeitung ohne Autorisierung nicht gelesen, kopiert, geändert, gespeichert oder entfernt werden können:

- Zwei-Faktor-Authentifizierung (mit Mindestlänge, regelmäßiger Änderung und strenger Vertraulichkeit für verwendete Passwörter)
- SSH-Netzwerkprotokoll und VPN-Verbindung für den Zugriff auf die Plattforminfrastruktur
- Automatische Sperre, Abmeldung
- Berechtigungskonzepte (Beschränkung auf autorisierte Mitarbeiter auf Rollenbasis)
- Verschlüsselte Speichermedien
- Nachverfolgung unerlaubter Aktivitäten/Zugriffe
- Verkapselung sensibler Systeme durch separate Netzwerkbereiche
- Firewall, regelmäßig aktualisierte Antiviren-Programme
- Dokumentierte Richtlinie zur Zugriffskontrolle

1.3. Trennungsgebot

Maßnahmen, um zu gewährleisten, dass die aus verschiedenen Anlässen erfassten Daten getrennt verarbeitet und infolgedessen von anderen Daten und Systemen abgesondert werden, um so eine ungeplante Verarbeitung dieser Daten aus anderen Gründen unmöglich zu machen:

- Berechtigungskonzepte
- Verschlüsselte Speicherung personenbezogener Daten
- Trennung der Clients innerhalb der Software
- Trennen von Test- und Produktionssystemen
- Geografische Verteilung: Ressourcen werden über mehrere Datenzentren mit verschiedenen Netzwerken verteilt. Grundsätzliche Einbindung der Redundanz in die Infrastruktur.

1.4. Pseudonymisierung

Maßnahmen zur Reduzierung personenbezogener Hinweise während der Datenverarbeitung in einem Maß, dass der persönliche Bezug zur betroffenen Person ohne weitere Informationen unmöglich ist. Alle zusätzlichen Informationen müssen demzufolge getrennt vom Nickname aufbewahrt werden:

- Hashwert-Funktion

1.5. Auftragskontrolle

Maßnahmen, um zu gewährleisten, dass im Falle der Auftragsverarbeitung personenbezogener Daten die Daten streng im Einklang mit den Anweisungen des für die Verarbeitung Verantwortlichen verarbeitet werden:

- Anweisungen des Auftraggebers
- Überwachung der Vertragsausführung
- Für alle Mitarbeiter geltende interne Richtlinien

2. Maßnahmen zur Gewährleistung der Integrität

2.1. Kontrolle der Datenübertragung

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten ohne Erlaubnis während der elektronischen Übertragung oder dem Transport nicht gelesen, kopiert, geändert oder entfernt werden können und dass die Überprüfung und Feststellung möglich ist, zu welcher Stelle die Übermittlung personenbezogener Daten geplant ist:

- Übermittlung von Daten über verschlüsselte Datennetzwerke (https)
- Umfangreiche Aufzeichnungsprozesse
- Kein Datenverkehr außerhalb der EU

2.2. Eingabekontrolle

Maßnahmen, um zu gewährleisten, dass nachträglich geprüft und festgestellt werden kann, von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, geändert oder aus diesen entfernt wurden:

- Speicherung personenbezogener Daten für einen begrenzten Zeitraum von 13 Monaten nach Kontoschließung, außer ausdrücklich anderweitig angeordnet

- Datensatzbewertungssysteme (bei Anwendungsschnittstellen werden IP, Datum, URL und Methode aufbewahrt. Bei grafischen Benutzerschnittstellen werden für jede Sitzung die IP-Adresse und HTTP-Protokolle für alle Anfragen aufbewahrt).
- Dokumentationen zu Anforderungen werden aufbewahrt.

3. Maßnahmen zur Gewährleistung von Verfügbarkeit und Kapazität

3.1. Verfügbarkeitskontrolle

Maßnahmen, um zu gewährleisten, dass die personenbezogenen Daten vor unbeabsichtigter Zerstörung oder unbeabsichtigtem Verlust geschützt sind:

- Datensicherung
- Replizierung der Datenbanken in mehrere Systeme
- Geografische Verteilung: Ressourcen werden über mehrere Datenzentren mit verschiedenen Netzwerken verteilt. Grundsätzliche Einbindung der Redundanz in die Infrastruktur
- Unterbrechungsfreie Stromversorgung
- Brandmeldesystem
- Klimatisierungssystem
- Alarmsystem

3.2. Schnelle Wiederherstellbarkeit

Maßnahmen zur Gewährleistung einer schnellen Wiederherstellung der Verfügbarkeit und Zugänglichkeit von Daten im Falle eines physischen oder technischen Vorfalls.

- Vorfallsmanagement
- Disaster Recovery-Plan und Notfallplan
- Automatische Umschaltung der Datenbankserver
- Datensicherung
- Regelmäßige Überprüfung der Datenwiederherstellbarkeit

4. Maßnahmen für die regelmäßige Bewertung der Sicherheit der Datenverarbeitung

Maßnahmen, um eine sichere Datenverarbeitung in Einklang mit den Gesetzen zu gewährleisten.

- Datenschutzmanagement
- ISO 27001-Zertifizierung und regelmäßige Neuzertifizierung
- Externe Penetrations- und Sicherheitstests (einschließlich Anwendung einer Bug Bounty-Plattform)
- Prozedur bei Datenschutzverletzungen
- Dokumentation der Kundenanweisungen