Technisch organisatorische Maßnahmen (TOM)- Datenschutz gemäß DSGVO

Der Organisation
Web Inclusion GmbH
Gartenstraße 12c
97276 Margetshöchheim

Stand 18.09.2023

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

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	Organisatorische Maßnahmen
● Manuelles Schließsystem ● Sicherheitsschlösser ● Türen mit Knauf Außenseite	● Schlüsselregelung / Liste ● Empfang ● Sorgfältige Auswahl von Reinigungspersonal

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
● Login mit Benutzername und Passwort ● Anti-Virus-Software auf allen Rechner mit Zugriffsberechtigung ● Firewall auf allen Rechner mit Zugriffsberechtigung ● Zwei Faktor Authentifizierung	● Verwalten von Benutzerberechtigungen ● Erstellen von Benutzerprofilen ● Zentrale Passwortvergabe ● Richtlinie „Starkes Passwort“ ● Allgemeine interne Richtlinie zu Datenschutz und Sicherheit

1.3 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.

Technische Maßnahmen	Organisatorische Maßnahmen
• Sichere Aufbewahrung von Datenträgern; für Unberechtigte nicht zugänglich. • Keine Speicherung von persönlichen Daten außerhalb der gesicherten Serverumgebung	• Einsatz von Berechtigungskonzepten • Minimale Anzahl von Administratoren • Verwaltung der Benutzerrechte durch Administratoren

1.4 Trennungskontrolle

Die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, ist zu garantieren!

Technische Maßnahmen	Organisatorische Maßnahmen
• Trennung von Produktiv- und Testumgebung	• Steuerung über Berechtigungskonzepte • Festlegung von Datenbankrechten

1.5 Pseudonymisierung

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.

Technische Maßnahmen	Organisatorische Maßnahmen
● IP-Adressen werden direkt anonymisiert und liegen zu keinem Zeitpunkt vollständig vor (letzte Ziffer wird entfernt) ● Im Falle einer Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten Systemen	

1.6 Bearbeitung und Zugang des Source Code

Der Source Code der Anwendungen wird ausschließlich von internen Mitarbeitern ohne externe Beauftragung entwickelt. Updates werden zudem intern mit dem kompletten Entwicklungsteam besprochen und getestet.

Technische Maßnahmen	Organisatorische Maßnahmen
● Passwort-Schutz sowie Zwei Faktor Authentifizierung für alle Zugänge des Source Codes (Git)	● Strenge Limitierung des Zugriffs des Software-Codes auf Produktivservern auf die Führungsebene ● Überprüfung jedes Merge Request für Produktivsysteme nach dem 4-Augen Prinzip ● Programmierrichtlinen und IDE EInstellungen für sicheren Code

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

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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
● E-Mail-Verschlüsselung bei vertraulichen Informationen ● Verwendung von verschlüsselten Verbindungen wie sftp und https ● Protokollierung der Zugriffe	● Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. Löschfristen ● Übersicht regelmäßiger Abruf- und Übermittlungsvorgänge

2.2 Eingabekontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
● Anfertigung eines Protokolls bezüglich der Eingabe, Veränderung und Löschung von Daten in der Datenbank ● Manuelle Kontrolle der Protokolle	● Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können ● Nachvollziehbarkeit von Eingabe, Änderung und Löschung der Daten durch individuelle Benutzernamen ● Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten aus Basis eine Berechtigungskonzepts ● Klare Zuständigkeiten für Löschungen

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

3.1 Verfügbarkeitskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
● Feuer- und Rauchmeldeanlagen ● Feuerlöscher	● Backup & Recovery-Konzept über weitere Server von Drittanbietern ● Regelmäßige Tests der Datenwiederherstellung

3.2 Wiederherstellbarkeit

Maßnahmen, die die rasche Wiederherstellung der Verfügbarkeit von Daten nach deren zwischenzeitlichen Verlust oder Beschädigung gewährleisten.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Technische Maßnahmen	Organisatorische Maßnahmen
● Verfügbarkeit eines Notfall-RZ	● Notfallkonzept/Notfallplan ● Aufbewahrung der physischen Notfall Zugriffcodes für den Wechsel des Rechenzentrums an zwei Büro-Standorten (Würzburg und Leipzig)

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

4.1 Datenschutzmanagement

Technische Maßnahmen	Organisatorische Maßnahmen
● Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Berechtigung ● Eine Überprüfung der technischen Schutzmaßnahmen intern sowie die Akkreditierung unserer externen Dienstleister wird mindestens jährlich durchgeführt	● Interner Datenschutzbeauftragter Tobias Greiner, Web Inclusion GmbH, tobias@eye-able.com ● Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet ● Die Organisation kommt den Informationspflichten nach Art. 13 und 14 nach DSGVO nach

4.2 Incident-Response-Management

Technisch-organisatorische Maßnahmen zur Umsetzung datenschutzrechtlicher Vorgaben, d.h. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.
Data Privacy by Design and by Default

Technische Maßnahmen	Organisatorische Maßnahmen
● Einsatz von Firewalls auf allen internen Rechnern und regelmäßige Aktualisierung ● Einsatz von Spamfiltern über den E-Mail Provider ● Einsatz von Virenscannern auf allen internen Rechnern und regelmäßige Aktualisierung	● Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen ● Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen ● Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem ● Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Technisch-organisatorische Maßnahmen zur Umsetzung datenschutzrechtlicher Vorgaben, d.h. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.
Data Privacy by Design and by Default

Technische Maßnahmen	Organisatorische Maßnahmen
● Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind ● Bei Bedarf einfache Ausübung des Widerrufrechts durch technische Maßnahmen	

4.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass im Rahmen der Auftragsdatenverarbeitung personenbezogenen Daten nur nach Weisung des Auftraggebers verarbeitet werden (können)!

Technische Maßnahmen	Organisatorische Maßnahmen
	● Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation ● Auswahl des Auftragsnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit) ● Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln

Ausgefüllt durch

Name	Tobias Greiner
Funktion	Chief Technology Officer
Rufnummer	+49 159 06705421
Email	tobias.greiner@eye-able.com

Ort, Datum
Würzburg, 16.09.2023