WIKANDO GmbH
Schießgrabenstr. 32, 86150 Augsburg

Technisch-Organisatorische Maßnahmen gem. Art. 32 DSGVO

Wikando GmbH
Peter Kral (Geschäftsführer)
Schießgrabenstraße 32
86150 Augsburg
Telefon: 0821 66609000
E-Mail: info@fundraisingbox.com

Stand: 22.11.2023

Inhaltsverzeichnis **2**

1. Einleitung und Rahmenbedingungen **4**
1.1 Einleitung 4
1.2 Unternehmen / Behörde 4
1.3 Externer Datenschutzbeauftragter 5

2. Technisch-Organisatorische Maßnahmen **6**
2.1 Gewährleistung der Vertraulichkeit 6
2.1.1 Zutrittskontrolle 6
2.1.2 Zugangskontrolle 6
2.1.3 Zugriffskontrolle 7
2.1.4 Trennungskontrolle 8
2.2 Gewährleistung der Integrität 9
2.2.1 Weitergabekontrolle 9
2.2.2 Eingabekontrolle 9
2.3 Pseudonymisierung und Verschlüsselung 10
2.3.1 Pseudonymisierung 10
2.3.2 Verschlüsselung 10
2.4 Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit 11
2.4.1 Verfügbarkeit (der Daten) 11
2.4.2 Belastbarkeit (der Systeme) 11
2.4.3 Wiederherstellbarkeit (der Daten / der Systeme) 12
2.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung 13
2.5.1 Auftragskontrolle 13
2.5.2 Datenschutz-Management 13
2.5.3 Incident-Response-Management 14
2.5.4 Datenschutzfreundliche Voreinstellungen 14

1. Einleitung und Rahmenbedingungen

1.1 Einleitung

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die Technischen und Organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1.2 Unternehmen / Behörde

Die folgenden Festlegungen repräsentieren das Datenschutzkonzept der

Wikando GmbH
Peter Kral (Geschäftsführer)
Schießgrabenstrasse 32
86150 Augsburg
Telefon: 0821 66609000
E-Mail: info@fundraisingbox.com

1.3 Externer Datenschutzbeauftragter

Datenschutzberatung Mundanjohl
Andreas Mundanjohl
Zeller Strasse 30
73101 Aichelberg
Deutschland
Telefon: 0821 90782120
E-Mail: datenschutz@mundanjohl.de

2. Technisch-Organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen Folgendes ein:

2.1 Gewährleistung der Vertraulichkeit

2.1.1 Zutrittskontrolle

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

Maßnahmen:

- Prüfung und Bewertung des mobilen Arbeitsplatzes

2.1.2 Zugangskontrolle

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

Maßnahmen:

- Allgemeine Richtlinie Datenschutz und / oder Sicherheit
- Anleitung „Manuelle Desktopsperre“
- Anti-Viren-Software
- Anwendung einer 2-Faktor-Authentifikation
- Automatische Desktopsperre
- Einsatz einer Software-Firewall
- Einsatz von VPN bei Remote-Zugriff
- Login mit Benutzername und Passwort

Mobile Device Policy

Passwortvergabe

Richtlinie „Sicheres Passwort“

Verschlüsselung von Notebooks / Tablet

Verwalten von Benutzerberechtigungen

Verwaltung der Rechte durch einen Systemadministrator

Zuordnung von Benutzerprofilen zu IT-Systemen

Zuordnung von Benutzerrechten

Authentifikation mit SSH Keys

Intrusion Detection Systeme

Richtlinie „Clean Desk“

Zugangssperre bei mehr als 3 Anmeldeversuchen

2.1.3 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.

Maßnahmen:

Datenträger Inventuren

Differenzierte Berechtigungen (Anwendungen)

Differenzierte Berechtigungen (Betriebssystem)

Differenzierte Berechtigungen (Daten)

Einsatz der minimalen Anzahl an Administratoren

Einsatz von Entsorgungsunternehmen für die Entsorgung von Datenträgern

Einsatz von schriftlichen Berechtigungskonzepten

Löschprotokoll

Protokollierung der Ausgabe von Datenträgern

Richtlinien zur Entsorgung / Vernichtung von nicht mehr gebrauchten Datenträgern

Verwaltung der Benutzerrechte durch Administratoren

Manuelle Protokollauswertung

2.1.4 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.

Maßnahmen:

Festlegung von Datenbankrechten

Steuerung über ein Berechtigungskonzept

Trennung von Produktiv- und Testumgebung

Logische Mandantentrennung (softwareseitig)

2.2 Gewährleistung der Integrität

2.2.1 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.

Maßnahmen:

- Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- Dokumentation der Löschfristen
- Einsatz von VPN-Technologie
- Email-Verschlüsselung

2.2.2 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.

Maßnahmen:

- Klare Zuständigkeiten für die Löschung von Daten
- Technische Protokollierung der Löschung von Daten
- Verwendung von Zugriffsrechten
- Manuelle Kontrolle der Protokolle
- Nachvollziehbarkeit der Bearbeitung von Daten durch individuelle Benutzernamen
- Vergabe von Rechten zur Bearbeitung von Daten
- Übersicht über die Nutzung der Programme zur Bearbeitung von Daten

2.3 Pseudonymisierung und Verschlüsselung

2.3.1 Pseudonymisierung

Maßnahmen, die eine Pseudonymisierung von Daten gewährleisten.

Maßnahmen:

- Interne Anweisung, personenbezogene Daten nach Ablauf der Löschfrist mindestens zu pseudonymisieren, oder zu löschen

2.3.2 Verschlüsselung

Maßnahmen, die eine Verschlüsselung von Daten gewährleisten.

Maßnahmen:

- Verschlüsselter Zugriff auf Datenbanken von Kunden
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Verschlüsselter Zugriff auf externe SaaS Lösungen
- Verschlüsselung der Daten der Fundraisingbox während Transport und Speicherung mit Schlüsselhoheit bei Wikando

2.4 Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

2.4.1 Verfügbarkeit (der Daten)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Verfügbarkeit von Daten.

Maßnahmen:

- Backup & Recovery-Konzept
- Betrieb von Hochverfügbarkeits-Webservern
- Datensicherungskonzept vorhanden
- Monatliche Backups
- SLA mit Hosting Dienstleister
- Wöchentliche Backups
- Tägliche Backups
- 99,99% Verfügbarkeit der Server-Hardware
- Unterbrechungsfreie Stromversorgung (USV)

2.4.2 Belastbarkeit (der Systeme)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Belastbarkeit der Systeme.

Maßnahmen:

- Einsatz von Software Firewalls
- Einspielen von aktuellen Sicherheitsupdates auf allen Applikationsservern
- Einspielen von Sicherheitsupdates auf allen Entwicklersystemen
- Einsatz von Intrusion Detection Systemen

2.4.3 Wiederherstellbarkeit (der Daten / der Systeme)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Wiederherstellbarkeit von Daten und Systemen.

Maßnahmen:

- Restore von Datenbanken und Dateisystemen aus dem Backup der Webserver
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Existenz eines Notfallplans

2.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

2.5.1 Auftragskontrolle

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

Maßnahmen:

- Abschluss der notwendigen Auftragsverarbeitungsvereinbarungen
- Abschluss der notwendigen Standard-Vertragsklauseln
- Regelung zum Einsatz von Subunternehmern
- Überprüfung des Schutzniveaus des Auftragnehmers (initial)
- Überprüfung des Schutzniveaus des Auftragnehmers (kontinuierlich)
- Sicherstellung der Vernichtung von Daten nach Beendigung eines Auftrags
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das spezielle Geheimhaltungsvorschriften

2.5.2 Datenschutz-Management

Maßnahmen, die gewährleisten, dass Methoden evaluiert wurden, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, organisieren, steuern und kontrollieren.

Maßnahmen:

- Bestellung eines externen Datenschutzbeauftragten
- Bereitstellung eines internen Datenschutz Teams
- Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz
- Durchführung von Datenschutz Folgenabschätzungen (bei Bedarf)
- Einhaltung der Informationspflichten gemäß Art. 13 DSGVO
- Einhaltung der Informationspflichten gemäß Art. 14 DSGVO

Einsatz von Softwarelösungen für Datenschutz-Management

Evaluierung eines formalisierten Prozesses zur Bearbeitung von Auskunftsanfragen

Regelmäßige Sensibilisierung der Mitarbeiter zum Datenschutz

Schulung der Mitarbeiter zum Datenschutz

Überprüfung der Wirksamkeit der TOMs (mind. jährlich durchgeführt)

Verpflichtung der Mitarbeiter auf das Datengeheimnis

Zugriffsmöglichkeiten für Mitarbeiter zu den Regelungen zum Datenschutz (Wiki / Intranet)

2.5.3 Incident-Response-Management

Maßnahmen, die gewährleisten, dass Sicherheitsvorfällen vorgebeugt werden kann oder im Falle von bereits eingetretenen Sicherheitsvorfällen, dass Daten und Systeme geschützt werden können und eine schnelle Analyse und Behebung des Sicherheitsvorfalls durchgeführt werden kann.

Maßnahmen:

Dokumentation von Sicherheitsvorfällen

Dokumentierter Prozess zur Meldung von Sicherheitsvorfällen

Einbindung von Datenschutzbeauftragten in Sicherheitsvorfälle

Einbindung von externen Dienstleistern zur Untersuchung und Behebung von Datenpannen

Einsatz von Firewall und deren regelmäßige Aktualisierung

Einsatz von Virenscanner und deren regelmäßige Aktualisierung

Klarer Prozess zur Regelung von Verantwortlichkeiten bei Sicherheitsvorfällen

Einsatz von Logging Systemen

2.5.4 Datenschutzfreundliche Voreinstellungen

Maßnahmen, die gewährleisten, dass bereits durch die entsprechende Technikgestaltung (privacy by design) und Werkseinstellungen (privacy by default) einer Software vorab ein gewisses Datenschutzniveau herrscht.

Maßnahmen:

Personenbezogene Daten werden nur zweckerforderlich erhoben