FUNDRAISINGBOX

Technische und organisatorische Maßnahmen
zur Einhaltung und Sicherheit der Verarbeitung

V1_24.01.2022

Einführung

Nach EU-DSGVO ist der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Da uns der vertrauensvolle Umgang mit Ihren Spender*innen Daten wichtig ist, haben wir alle Ansprüche der EU-DSGVO in unseren Betriebsablauf integriert und prüfen hierzu in regelmäßigen Abständen unsere Prozesse um Ihre personenbezogenen Daten sicher zu verarbeiten.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

Inhaltsverzeichnis

01

Kontrollen unserer Infrastruktur

Um eine optimale Sicherheit zu gewährleisten, arbeitet die Wikando GmbH mit Hosting Anbietern zusammen. Durch deren Schutzmaßnahmen, Normen und Zertifizierungen Ihre personenbezogenen Daten geschützt verarbeitet werden können. Darüber hinaus haben wir weitere Kontrollen unserer Infrastruktur implementiert.

- Zwei-Faktor-Authentifizierung
- Firewall limitiert die Port-Freigabe auf die minimal notwendigen Dienste
- Zugriff auf Serverumgebungen erfolgt über einen passwortabgesicherten, verschlüsselten SSH-Zugang sowie über spezielle Gateway Server, die nur im Bedarfsfall gestartet werden
- Einsatz von Anti-Viren-Software
- Einsatz von VPN-Verbindungen bei Remote-Zugriff
- Automatische Desktopsperre
- Datenträgerinventuren
- Protokollierungen von Zugriffen
- Trennung von Produktiv- und Testumgebung
- Intrusion Prevention System (IPS)

02

Richtlinien und Prozesse

Um alle Betriebsabläufe der Wikando GmbH datenschutzkonform zu gestalten, haben wir ein umfangreiches Datenschutz-Management implementiert. Somit gibt es einheitliche interne Prozesse zu den Verfahrensweisen, Regelungen, Verantwortlichkeiten, sowie den regelmäßigen Prüfungen.

- Allgemeine Richtlinie zu Datenschutz und Sicherheit
  Mobile Device Policy
- Regelmäßige Sensibilisierung und Schulung der
- Mitarbeitenden zum Datenschutz
- Richtlinie zur Ausgabe und Vernichtung von Datenträgern
- Löschkonzept

Zur Verwaltung der Zugänge der Mitarbeitenden, haben wir ein Rollen-Rechte-Konzept. Jeder Mitarbeitende erhält Zugänge ausschließlich nach dem Prinzip des geringsten Privilegs (engl. “principle of least privilege”). Somit ist ausschließlich der Zugriff auf notwendige Systeme, sowie mit den entsprechenden zugewiesenen Berechtigungen der auszuübenden Tätigkeit möglich. Die Erteilung der Berechtigungen erfolgt in einem dokumentierten Genehmigungsverfahren. Das Erfordernis der Berechtigung wird regelmäßig überprüft.

- Vertraulichkeitsverpflichtungen
- Richtlinie zur Passwortverwaltung und -vergabe
- Verwaltung der Benutzerrechte durch
- Systemadministrator
- Differenzierte Berechtigungen für Daten,
  Betriebssystem und Anwendungen

03

Verschlüsselung

Zur Verschlüsselung setzt die Wikando GmbH auf Verschlüsselungstechnologien, die dem Stand der Technik entsprechen. Sie besitzen ein Schutzniveau, das Ihren personenbezogene Daten und den damit verbunden Verarbeitungstätigkeiten angemessen ist.

- Zugriff auf das Rechenzentrum über VPN-, https- oder TLS-Verbindung mit Zwei-Faktor-Authentisierung
- Einzelpersonen: personenbezogene Daten der Nutzer über Internet, abgesichert mit Verschlüsselungsverfahren nach dem Stand der Technik
- Mitarbeitende der Wikando: Verschlüsselte Verbindung mit Zwei-Faktor-Authentisierung und wo möglich One-Time-Password Verfahren
- Festplatten von Remote-Arbeitsplatz-Rechnern (Laptops) werden standardisiert nur vollverschlüsselt eingesetzt

04

Incident-Response-Management

Die Mitarbeitenden der Wikando GmbH sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers. Die Wikando GmbH hat einen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betriebliche Prozesse. Zudem haben wir Prozesse zum Schwachstellen- und Vorfalls-management integriert.

- Regelmäßige SSL Scans und Updates
- Regelmäßige Sicherheitsüberprüfungen der Server und Endgeräte
- Pentest-Audit durch eine Fachfirma
- Audits und Code-Reviews

05

Gewährleistung der Verfügbarkeit und Belastbarkeit

Wikando trifft für die Auftragsdatenverarbeitung in ihrer Server-Infrastruktur Maßnahmen für eine Systemstabilität, die dem Anspruch der großen Anzahl von Kunden und Spenden einer zuverlässigen und zeitgerechten Verarbeitung der Daten gerecht wird. Wikando legt die Speicher-, Zugriffs- und Leitungskapazitäten der Systeme und Dienste so aus, dass sie auch an Tagen planerischer Spitzenbelastung ohne merkliche Verzögerung von Zugriffs- oder Übertragungszeiten genutzt werden können.

- Redundante und skalierbare Infrastruktur
- Tägliche Backups
- Ausfallsichere Energieversorgungssysteme
- Brand- und Hochwasserschutzmaßnahmen
- Backup- und Recoveryplan
- Prozesse zur Leistungsüberwachung
- Management der Sicherheitsinformationen und -ereignisse

06

Entwicklungs-sicherheit

Um eine sichere Weiterentwicklung unserer FundraisingBox zu gewährleisten, haben wir interne Prozesse zur Entwicklung implementiert.

- Security-by-Design-Ansatz
- Automatische und manuelle Tests
- Code-Reviews und -Änderungen
- Peer-Review

FUNDRAISINGBOX

www.fundraisingbox.com

V1_24.01.2022