Technische und organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DSGVO

Organisation:
openPetition gGmbH
Stand:
24.07.2018
Verfasser:
Jörg Mitzlaff
Geschäftsführer openPetition gGmbH
Greifswalder Str. 4, 10405 Berlin

1 Technische und organisatorische Maßnahmen

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.

Die openPetition gGmbH erfüllt diesen Anspruch durch folgende Maßnahmen:

1.1 Zutrittskontrolle

Personenbezogene Nutzerdaten werden ausschließlich auf Servern im Rechenzentrum von Hetzner verarbeitet.
Besucher, Dienstleister und Lieferanten sind nur in Begleitung im Büro.
Die Bürotür ist zu jedem Zeitpunkt verschlossen, der Vermieter hat nachts und am Wochenende einen Wachschutz.
Der Vermieter verwaltet das Schließsystem. Es werden Schlüssel an die Mitarbeiter ausgegeben.
Es gibt eine Vorschrift, wie das Büro gegen Einbruch beim Verlassen zu sichern ist.

1.2 Zugangskontrolle

Die Regeln zur Generierung und Anwendung von Passwörtern ist in den Datenschutzrichtlinien hinterlegt.
Je nach Sicherheitsstufe werden verschiedene Passwortregelungen verwendet. Sie sind in den Datenschutzrichtlinien hinterlegt.

Nach wenigen Minuten ohne Aktivität, aktiviert sich an allen Arbeitsplätzen der automatische Bildschirmschoner mit Passwortschutz.
Für die Anwendungssoftware werden nur personalisierte Zugänge und Passwörter verwendet, allein schon aus Gründen der Nachvollziehbarkeit von Handlungen.
Der Administrator prüft regelmäßig Logs nach Auffälligkeiten.
Der Zugriff auf die Server erfolgt über ein Public-Key-Verschlüsselungsverfahren. Der Zugang ist auf die Mitarbeiter mit der Rolle Administration beschränkt.
Datenträger von Arbeitsplatzrechnern mit personenbezogenen Daten werden auf Dateisystem-Ebene verschlüsselt.
In den Büros sind keine Server und Rechner mit personenbezogenen Daten installiert. Mobile Arbeitsplatzrechner werden im Normalfall nicht im Büro gelagert.
Keine Standard Ports für SSH Verbindungen.
Einsatz von Viren-Schutzprogrammen auf allen Arbeitsplatzrechnern.
Kontrolle der Einhaltung von Standards für sichere Programmierung nach dem 4-Augen Prinzip.
Trennung Produktiv- und Testsystem.
Regelmäßige Prüfung auf bekannte Angriffsvektoren.
Die Webserver-Installation hat nur auf statische Dateien Zugriff.
Restriktive Konfiguration von Webservern.
Minimierung des Einsatzes externer Softwarebibliotheken und Frameworks.
Automatisierte Aktualisierung von Serverbetriebssystem-Updates. Zeitnaher Serverreboot nach Kernel Updates.

1.3 Zugriffskontrolle

Es gibt die Rollen Redaktion, Technik, Administration und Geschäftsführung.
Die Rollen haben je nach Aufgabenprofil zu spezifischen, personenbezogenen Daten, Lese-, Schreib- und Löschrechte. Die Rechte werden von der Anwendungssoftware durchgesetzt.
Nur der Geschäftsführer und Administratoren können Geräte administrieren. Die Administration von Servern und Arbeitsplatzrechnern sind getrennt.
Der Geschäftsführer erteilt Berechtigungen. Das Rechte- und Rollenkonzept ist Teil des Verzeichnisses von Verarbeitungstätigkeiten.
Analoge personenbezogene Daten fallen im Büro nicht an. Werden uns analoge personenbezogene Daten zugesendet, werden sie geschreddert.
Nicht mehr benötigte Datenträger werden physisch zerstört.
Es gibt keine externen Datenträger mit personenbezogenen Daten. Backups erfolgen auf eigenen Servern.
Zu jedem Zeitpunkt ist die Anzahl der abrufbaren personenbezogenen Datensätze durch die Anwendungssoftware beschränkt.

1.4 Weitergabekontrolle

Personenbezogene Daten können über einen Webdienst exportiert werden.
Die Daten sind über ein Nutzeraccount gesichert und werden per SSL Verschlüsselung übertragen.
Es gibt drei Schutzklassen: interne Daten, personenbezogene Daten und geheime Daten wie Passwörter und private Keys.
Die Datenschutzrichtlinie regelt, welche Daten nur verschlüsselt übertragen werden dürfen.
Per Email übertragene Daten werden 10 Jahre lang aufbewahrt.
Durch Firewalls werden die möglichen Kommunikationskanäle auf unseren Servern beschränkt. Es werden die Serverlogs auf auffälligen Webanfragen geprüft und ggf. manuell blockiert.
Der Zugriff auf die Datenbank ist intern über eine verschlüsselte SSL Verbindung realisiert. Externer Datenbank Zugriff ist nur über eine gesicherte SSH Verbindungen möglich.

1.5 Eingabekontrolle

Nachvollziehbarkeit von Eingabe, Änderung und Ausblenden von personenbezogenen Daten durch individuelle Benutzerkonten und Verwendung eines Changelogs auf Anwendungsebene.
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts.

1.6 Auftragskontrolle

Von allen Auftragsdatenverarbeitern liegen ADV-Verträge vor.
Hostingprovider Hetzner Online ist nach DIN ISO/IEC 27001 zertifiziert.
Die Server sind Root-Serversysteme mit exklusivem root Zugang.
Dienstleistende sind vertraglich an die Befolgung der datenschutzrechtlichen Anweisungen gebunden.
Mitarbeiter sind vertraglich und durch eine Vertraulichkeitserklärung an die Befolgung der datenschutzrechtlichen Anweisungen gebunden.

1.7 Verfügbarkeitskontrolle

Backups des Server-Dateisystems erfolgen täglich. Die Datenbank wird in Echtzeit mit einem Master-Slave Verfahren repliziert.
Backups werden einmal im Quartal zurückgespielt und auf Korrektheit überprüft. Der Status der Datenbank-Replikation wird laufend überprüft.

1.8 Trennungsgebot

Kundendaten werden durch spezifische Datenbankattribute von anderen Datensätzen unterschieden.
Das Datenbankmodell sichert die Trennung von inhaltlich unterschiedlichen Daten.
Kundendaten unterliegen dem gleichen Rollen- und Rechtemodell für personenbezogene Daten.

Test- und Produktivsysteme liegen auf verschiedenen physischen Servern.

1.9 Organisation (Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung)

Der Verantwortliche für die datenschutzkonforme Verarbeitung von Daten nach Artikel 24 DSGVO ist bei openPetition der geschäftsführende Gesellschafter Jörg Mitzlaff.
Der Verantwortliche für die datenschutzkonforme Verarbeitung von Daten nach Artikel 24 DSGVO ist studierter Diplom-Informatiker und hat eine langjährige, einschlägige Berufserfahrung mit informationsverarbeitenden Systemen.
Der Nachweis über die DSGVO-konforme, regelmäßige Verarbeitung personenbezogener Daten nach Art. 30 DSGVO liegt digital als Google-Drive Dokument vor und wird laufend aktualisiert.
Mitarbeiter werden im Umgang mit personenbezogenen Daten geschult. Mitarbeiter protokollieren die Kenntnisnahme der Datenschutzrichtlinien und der Vertraulichkeitsverpflichtung für Mitarbeiter von openPetition.
Das Datenschutzkonzept fasst die Einzelmaßnahmen Verzeichnis von Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzung für neue Produkte und Dienstleistungen, Vertragsmanagement für Auftragsdatenverarbeitung, Datenschutzrichtlinien und Vertraulichkeitsverpflichtung von Mitarbeitern, das Management für die Wahrnehmung von Betroffenenrechten und das Management für die Meldung von Datenschutzverstößen an einem Ort zusammen.
Die Entwicklung orientiert sich am BSI Leitfaden zur Entwicklung sicherer Webanwendungen.
Das Dokument Datenschutzrichtlinien und Vertraulichkeitsverpflichtung für Mitarbeiter von openPetition wird regelmäßig an die neuen technischen Anforderungen im Umgang mit personenbezogenen Daten angepasst.
Datenminimierung personenbezogener Daten ist ein Design-Kriterium bei der Weiterentwicklung und Wartung der Anwendungssoftware.
Der Geschäftsführer ist zugleich der Informationssicherheitsbeauftragte. Grundlage für das Informationssicherheits-Management sind die IT-Grundschutzkataloge des BSI. Das Informationssicherheits-Management fasst die Einzelmaßnahmen Schulung zum sicheren Umgang mit der IT-Infrastruktur, Verwaltung der Zugänge und Zugriffsrechte, Maßnahmenkatalog für die Entwicklung sicherer Webanwendungen, Maßnahmenkatalog für die Absicherung von Standard-Hardware und -Software, Maßnahmenkatalog für Ausfälle und Sicherheitsvorfälle an einem Ort zusammen.

1.10 Datenschutzfreundliche Voreinstellungen

Benutzer haben jederzeit die Möglichkeit, mit wenigen Klicks die Einwilligung in die Speicherung personenbezogener Daten zu widerrufen und ihre Daten zu löschen.
Benutzer haben jederzeit die Möglichkeit, mit wenigen Klicks Auskunft über die von ihm gespeicherten Daten zu erhalten.