Technische und organisatorische Maßnahmen der makandra GmbH nach Art. 32 DSGVO

Stand: 13.08.2018

Inhaltsverzeichnis

Einleitung

Die makandra GmbH hat geeignete technische und organisatorische Maßnahmen getroffen, um den Schutz der Rechte der betroffenen Personen und ein mit der Verarbeitung personenbezogener Daten verbundenem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet werden. Diese technischen und organisatorischen Maßnahmen umfassen:

Vertraulichkeit

Zutrittskontrolle

Es ist ein mehrstufiges Zutrittskonzept im Einsatz:

- Der Zutritt zum aiti-Park (Bürogebäude) ist nur mit einem aiti-Park-Ausweis möglich. Es ist aiti-Park-seitig dokumentiert, welche Karte welche Türe öffnen kann. Alle makandra Mitarbeiter haben die gleichen Berechtigungen.
- Der Werkschutz begeht regelmäßig alle Räumlichkeiten.
- Der Zutritt zu den Räumlichkeiten der IT (Server) ist nur für einen eingeschränkten Personenkreis möglich. Der Zutritt zu den Serverräumen ist nochmals eingeschränkt.

Zugangskontrolle

- Eine automatische Sperrung erfolgt bei Rechnern innerhalb der Domäne.
- Alle Rechner innerhalb der Domäne sind verschlüsselt.
- Alle Mitarbeiter sind angehalten, zufallsgenerierte Passwörter zu verwenden und in einer verschlüsselten Form zu speichern.

Zugriffskontrolle

- Es ist ein Rollenkonzept im Einsatz. In einigen Fällen sind Rollen für Einzelpersonen definiert.
- Programmbasierte Berechtigungen werden aktuell individuell vergeben.

Trennungskontrolle

- Sämtliche Daten werden nur für die jeweiligen einzelnen Kunden separat in das System eingepflegt und verarbeitet. Die Datenspeicherung erfolgt separat je Kunde nach dessen Vertrag und dessen Weisungen.

Integrität

Weitergabekontrolle

- Alle extern über das Internet zugängliche Systeme sind ausschließlich über verschlüsselte Protokolle zugänglich.
- Für an die Mitarbeiter herausgegebene Geräte des Unternehmens gelten die genannten Sicherheitsanforderungen und Verschlüsselungstechniken. Daneben gilt eine separate IT-Benutzerordnung.

Eingabekontrolle

- Änderung von Daten werden systemintern protokolliert.
- Teilweise ist in anderen Systemen eine belegbezogene Protokollierung des angemeldeten Benutzers umgesetzt.
- Im Dateisystem wird anwendungsbezogen protokolliert, wer eine Datei angelegt oder zuletzt bearbeitet hat.
- Ausgewertet werden diese Protokolle nur im akuten Einzelfall.

Verfügbarkeit und Belastbarkeit der Dienste und Systeme sowie Wiederherstellung der Verfügbarkeit

- Es ist ein Backupkonzept im Einsatz und ein Notfallplan vorhanden.
- Es ist ein Vorgehen bei einem Informations-Sicherheitsvorfall definiert.

Verfahren zur regelmäßigen Überprüfung

- Regelmäßige interne Audits und weitere Maßnahmen.
- Verarbeitung personenbezogener Daten des Kunden in dessen Auftrag nur auf Grundlage eines Vertrags zur Auftragsverarbeitung nach Art. 28 Datenschutz-Grundverordnung.

Technische und organisatorische Maßnahmen der makandra GmbH für das Rechenzentrum nach Art. 32 DSGVO

Stand: 10.07.2019

Inhaltsverzeichnis

Einleitung

Im Rahmen der Leistungen der makandra GmbH 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, konkretisiert dieser Anhang die von der makandra GmbH getroffenen technischen und organisatorischen Maßnahmen des Rechenzentrums, die sich aus dem Leistungsvertrag in seinen Einzelheiten beschriebenen Datenverarbeitung ergeben, um ein dem Risiko angemessenes Datenschutzniveau zu gewährleisten.

Bei der makandra GmbH kommen grundsätzlich die folgenden Maßnahmen im Sinne des Art. 32 DSGVO. Eine rasche Wiederherstellung nach einem physischen oder technischen Zwischenfall ist gewährleistet.

Vertraulichkeit

Zutrittskontrolle

Es ist ein mehrstufiges Zutrittskonzept im Einsatz:

- Eingezäuntes Gelände
- Alarmanlagen
- Kameraüberwachung
- Zugang mittels personalisierter Chipkarten
- Manuelles Schließsystem mit Sicherheitsschlössern
- Protokollierung der Zutritte
- Regelmäßige Überprüfung von vergebenen Zutrittsrechten
- Schlüsselregelung
- Prozess zur Vergabe von Zutrittsrechten
- Zutritt externer Dienstleister nur in Begleitung eines Berechtigten oder per Videoüberwachung verfolgt
- Limitierung des Zutritts bestimmter Infrastrukturbereiche für Berechtigte (Carrier, Strom, etc.)
- Regelmäßige Kontrollgänge
- Einteilung in Sicherheitszonen
- Sicherheitsdienst vor-Ort

Übertragungs- und Transportkontrolle

Schützenswürdige Daten werden bevorzugt über Datenleitungen statt mittels physikalischem Transport übertragen, um das Risiko von Verlust oder einen Daten-Diebstahl über diese traditionellen Transportwege ausschließen zu können. Dabei kommt über öffentliche Kommunikationskanäle (wie Internet-Datenverkehr) eine verschlüsselte Datenübertragung zum Einsatz (z. B. per TLS, IPsec, SSL-VPN).

Zugangskontrolle

- Berechtigungskonzept für Zugänge zu Server-IT-Systemen
- Erstellen von Benutzerprofilen
- Passwortrichtlinie und geschützte Passwortvergabe
- Protokollierung von fehlgeschlagenen Zugriffsversuchen auf die Server-Systeme
- Prozess zur Rechtevergabe / zum Rechteentzug
- Rechtevergabe durch geschultes Personal
- Regelmäßige Überprüfung von Richtlinien auf Aktualität und Wirksamkeit
- Regelmäßige Überprüfung von Zugangsrechten auf die IT – Systeme
- Authentifizierung mit personifizierten SSH Keys
- Authentifizierung mit personifizierten Zugangsdaten

Zugriffskontrolle

- Berechtigungskonzept mit Minimalprinzip etabliert
- Etablierter Datenvernichtungs-/Datenlöschprozess
- Passwortrichtlinie inkl. Länge, Komplexität und Wechsel
- Regelmäßige Überprüfung der Richtlinien und Prozesse auf Aktualisierung
- Verwaltung von Benutzerrechte durch geschulte Systemadministratoren
- Berechtigungen nach Abteilungen und Zugriffserfordernissen
- Sicheres Löschen mittels Secure Erase
- Protokollierung von Zugriffen auf IT-Systeme

Integrität

- Berechtigungskonzept mit Minimalprinzip etabliert
- Etablierter Rechteprozess zur dokumentierten Vergabe/Entzug von Zugriffsrechten

- Verwaltung von Benutzerrechte durch geschulte Systemadministratoren

Verfügbarkeit und Belastbarkeit der Dienste und Systeme sowie Wiederherstellung der Verfügbarkeit

- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Backups auf physisch getrennten Geräten
- Monitoring aller relevanten Infrastrukturkomponenten und IT-Systeme
- Veträge zum Beliefern der Netzersatzanlage mit Kraftstoff 24/7/365
- Brandmeldeanlage mit Aufschaltung zur Feuerwehr
- Feuer- und Rauchmeldeanlagen
- Feuerlöschanlage (Argon/Stickstoff) im Serverraum vorhanden
- Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Klimaanlagen in Serverräumen
- Netzwerkanbindung über zwei separate Zuleitungen
- Einsatz von Datenspiegelung (RAID) für relevante IT-Systeme
- Einsatz redundanter Netzteile für relevante IT-Systeme
- Makandra legt alle IT-Systeme redundant aus, um Hardware-Ausfällen vorzubeugen. Ausgenommen sind ausdrücklich auf Kundenwunsch ohne Redundanz implementierte Systeme.
- Unterbrechungsfreie Stromversogung- USV Anlage relevante Infrastruktur und IT-Systeme
- Stromversorgung der Rechenzentrumsräume über zwei Zuleitungen
- Stromanbindung in Serverracks über zwei separate Zuführungen
- Regelmäßige Erstellung von Backups
- Regelmäßige Prüfung der Wiederherstellbarkeit von Backups
- Proaktiver Behandlung möglicher Fehlerquellen durch intensives Monitoring auch von Hardware-Komponenten

Verfahren zur regelmäßigen Überprüfung

- Regelmäßige interne Audits und weitere Maßnahmen
- Regelmäßige Sicherheits-Scans
- Bestellung eines Datenschutzbeauftragten