clockodo

Technische und organisatorische Maßnahmen nach Artikel 32 DSGVO

Die clickbits GmbH trifft folgende technische und organisatorische Maßnahmen, um bei der Verarbeitung personenbezogener Daten ein angemessenes Schutzniveau zu gewährleisten:

1. Pseudonymisierung

Die vom Nutzer in der Software eingegebenen sowie die vom System erhobenen Daten werden mit einer User-ID gespeichert. Diese ist ein Pseudonym für den jeweiligen Nutzer und lässt sich über eine weitere Tabelle dem Benutzernamen und der E-Mail-Adresse des Nutzers zuordnen. Als Benutzername können Pseudonyme statt der realen Namen genutzt werden.

2. Verschlüsselung

Datenträger in den Geschäftsräumen mit personenbezogenen Daten werden entsprechend dem Stand der Technik verschlüsselt. Der Zugang zu Server-Systemen sowie die Datenübertragung zwischen einzelnen Servern erfolgt über verschlüsselte Verbindungen.

Die Software ist durch den Kunden ausschließlich über verschlüsselte Internetverbindungen (https) nutzbar.

3. Gewährleistung der Vertraulichkeit

3.1. Zutrittskontrolle

Der Zutritt zu den Geschäftsräumen erfolgt über ein Schließsystem mit kontrollierter Schlüsselvergabe. Besucher dürfen die Geschäftsräume nur in Begleitung berechtigter Mitarbeiter betreten. Die Geschäftsräume sind teilweise mit einer Alarmanlage gesichert.

Die Zutrittskontrolle zum Rechenzentrum erfolgt auf Basis der technischen und organisatorischen Maßnahmen des Rechenzentrumsbetreibers Microsoft. Dieser hält internationale und branchenspezifische Compliancestandards ein, darunter ISO 27001. Mehr dazu unter https://www.microsoft.com/de-de/TrustCenter/

3.2. Zugangskontrolle

Die Anmeldung an IT-Systemen erfolgt über mindestens 12-stellige Kennwörter mit Sonderzeichen, Ziffer und/oder Klein- /Großbuchstaben. Sofern möglich sind die Login-Daten personenbezogen und nur dem jeweiligen Mitarbeiter bekannt.

Die IT-Systeme sind durch eine Firewall gesichert. Der administrative Zugriff auf die Serversysteme mit personenbezogenen Daten ist durch IP-basierte Firewallregeln nur aus dem Firmennetzwerk möglich.

Für Remote-Zugriffe werden personenbezogene VPN-Zugänge genutzt. Client-Rechner und Notebooks sowie deren Backups sind vollständig verschlüsselt.

3.3. Zugriffskontrolle

Für die Zugriffskontrolle sind differenzierte Berechtigungen nach dem Rollenkonzept eingerichtet. Die Freigabe von Daten erfolgt nur an berechtigte Personen. Zugewiesene Berechtigungen werden durch die Administratoren regelmäßig überprüft und bei Entfall der Notwendigkeit entzogen.

Nicht mehr benötigte Datenträger werden physisch zerstört.

3.4. Trennungskontrolle

Soweit die betrieblichen Abläufe eine getrennte Verarbeitung und Auswertung von Daten ermöglichen wird diese entsprechend eingerichtet. Produktiv- und Testsysteme nutzen generell getrennte Datenbanken. Für Kundendaten erfolgt eine logische Trennung auf Datenbankebene.

Der Zugriff auf Produktivsysteme wird soweit wie möglich eingeschränkt.

4. Gewährleistung der Integrität

4.1. Weitergabekontrolle

Zur Übertragung von Daten werden verschlüsselte Verbindungen entsprechend dem Stand der Technik eingesetzt. Die Remote-Einwahl in das interne Netzwerk erfolgt über VPN-Verbindungen.

4.2. Eingabekontrolle

Eingaben, Änderungen und Löschung von Produktivdaten sind nur durch Administratoren möglich. Diese Aktivitäten werden in Logdateien protokolliert. Die Logdateien werden bei Auffälligkeiten manuell auf unbefugte Aktivitäten kontrolliert.

5. Gewährleistung der Verfügbarkeit

Von Server-Systemen werden mehrmals täglich Backups durchgeführt. Die Verfügbarkeit der Server-Systeme wird außerdem durch Echtzeit-Spiegelung sichergestellt. Sicherungen werden zusätzlich räumlich getrennt an einem anderen Standort gespeichert.

Von Client-Rechnern werden täglich Backups erstellt. Auf allen Client-Rechnern ist Antiviren-Software installiert und wird fortlaufend aktualisiert.

Die Gewährleistung der Verfügbarkeit auf Ebene des Rechenzentrums erfolgt darüber hinaus auf Basis der technischen und organisatorischen Maßnahmen des Rechenzentrumsbetreibers Microsoft. Dieser hält internationale und branchenspezifische Compliancestandards ein, darunter ISO 27001. Mehr dazu unter https://www.microsoft.com/de-de/TrustCenter/

6. Gewährleistung der Belastbarkeit der Systeme

Um die Belastbarkeit der Systeme zu gewährleisten, setzen wir auf eine skalierbare Serverinfrastruktur mit Lastverteilung und ein umfangreiches Monitoring um Trends und Lastspitzen zu erkennen und rechtzeitig darauf zu reagieren. Die Cloud-Architektur des Rechenzentrums ermöglicht eine Erhöhung der Rechenkapazitäten innerhalb von wenigen Minuten, so dass auch spontan auftretende Lastspitzen abgefangen werden können.

Softwareänderungen werden vor der Produktivschaltung auf mögliche Auswirkungen auf die Serverleistung getestet.

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Die Administratoren sind in der Lage, die in 5. genannten Sicherungen zeitnah einzuspielen. Das Szenario wird in periodischen Abständen getestet.

Durch die Cloud-Architektur mit Lastverteilung führt ein physischer Defekt einzelner Systeme nicht zu einer Unterbrechung der Verfügbarkeit, diese werden automatisiert ausgetauscht.

Der Rechenzentrumsbetreiber stellt baugleiche Serversysteme an mehreren Standorten zur Verfügung, zwischen denen bei größeren Störungen innerhalb kurzer Zeit gewechselt werden kann.

8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag. Sie sind in einer gesonderten Vereinbarung dem Datengeheimnis verpflichtet.

Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnamen wird mindestens jährlich durchgeführt. Dabei erfolgt auch eine Beurteilung der Angemessenheit des Schutzniveaus und gegebenenfalls eine Anpassung auf den aktuellen Stand der Technik, beispielsweise eine Umstellung auf neuere Verschlüsselungsverfahren.