TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

(TOM)

Übersicht der technisch-organisatorischen Maßnahmen

Gemäß Art. 32 Abs. 1 DSGVO ist Verantwortlicher 1 verpflichtet, 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 geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Weiterhin ist Verantwortlicher 1 verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen die Rechte der betroffenen Personen zu schützen, sowie dafür zu sorgen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. (Art. 24 DSGVO „Privacy by Design, By Default“)

Die nachfolgende Darstellung dient dazu, einen Überblick zu geben, welche Maßnahmen Verantwortlicher 1 ergreift, um die Anforderungen der Art. 24 und Art. 32 DSGVO umzusetzen. Die Übersicht richtet sich nach der Struktur des Art. 32 Abs.1 DSGVO.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

a) Zutrittskontrolle

Die Kanzleiräume des Verantwortlichen 1 sind umfassend durch Einlasskontrollen und Sicherungsmechanismen gesichert, um einen unbefugten Zutritt zu Datenverarbeitungsanlagen zu verhindern (u.a. Alarmanlage, Wachdienst, Protokollierung des Zutritts usw.). Ein Zutritt ist nur autorisierten Mitarbeitern gestattet. Darüber hinaus sind die Büroräume des Verantwortlichen 1 gesichert u.a. durch Schlüssel.

b) Zugangskontrolle

- Verantwortlicher 1 setzt sichere und komplexe Kennwörter ein, um eine unbefugte Systembenutzung auszuschließen.
- Alle Daten im Zusammenhang mit den Hinweisen und deren Kommunikation werden Ende-zu-Ende verschlüsselt.

- Die Datenbanken werden verschlüsselt durch AES-256 Verschlüsselung.
- 2-Faktor-Authentifizierung für die Plattform.
- Es wird eine Firewall eingesetzt und es besteht ein umfassender Maleware-Schutz auf Arbeitsplatzrechnern und Servern.
- Verschlüsselung der Festplatten.
- Technische Sperre des Arbeitsplatzes bei Nicht-Aktivität.
- TLS-Verschlüsselung (Transport Layer Security) auf der Plattform.

c) Zugriffskontrolle

Mit diesen Maßnahmen soll verhindert werden, dass die in gemeinsamer Verantwortung verarbeiteten Daten nicht unbefugt gelesen, kopiert, geändert oder gelöscht werden. Die zur Nutzung von IT-Systemen Berechtigten dürfen ausschließlich auf die ihrer Zugriffsberechtigungen unterliegenden Daten zugreifen.

Mittels Berechtigungskonzepten (eingeschränkte Gruppenberechtigungen für Mitarbeiter) wird sichergestellt, dass Mitarbeiter nur auf die Daten, Dateien und Datenträger zugreifen können, die ihren Berechtigungen entsprechen. Differenzierte Berechtigungen auf verschiedenen Ordnern und Laufwerken sind eingerichtet. Die Mitarbeiter werden angehalten, Daten in Papierform sicher aufzubewahren und eine „Clean Desk Policy“ umzusetzen. Es besteht ein gelebtes Rechte- und Rollenkonzept für Mitarbeiter. Nur zuständige Mitarbeiter haben Zugriff auf diese Daten.

d) Trennungskontrolle

Die Datenbanken der jeweiligen Kunden werden getrennt administriert.

- Mehr-Mandantenfähigkeit.
- Getrennte Speicherung der Kundendaten.
- Trennung von Entwicklungs-, Test- und Produktivsysteme.

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Daten auf der Plattform werden verschlüsselt. Dadurch können die verschlüsselten Daten in der Plattform nicht durch Dritte de-pseudonymisiert bzw. es kann kein Personenbezug hergestellt werden.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

a) Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch eine industrieübliche SSL-Verschlüsselung. Zudem besteht eine Verschlüsselung der Endgeräte.

b) Eingabekontrolle

Modifikationen durch Veränderungen, Einfügungen und Löschungen werden in einem Index der Plattform revisionssicher protokolliert. Eine Löschung der Hinweise und des entsprechenden Index ist nur nach Durchlaufen des Vier-Augen-Prinzips (Manager + Admin oder Admin + Admin) möglich. Modifikationen durch den Verpflichteten stehen nur dem verantwortlichen Asset-Owner nach einem Vier-Augenprinzip zu und werden protokolliert.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

a) Verfügbarkeitskontrolle

Es werden täglich Back-ups von der Plattform angefertigt, um einen Verlust der Daten zu minimieren. Wir setzten einen industrieüblichen Virenschutz ein. Die vom Verantwortlichen 1 eingesetzten Host-Provider (ISO 27001 Zertifiziert) setzen eine umfassende USV ein und weitere Schutzmaßnahmen um (Firewall, Meldewege und Notfallpläne).

b) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Eine Wiederherstellung der Daten aus dem Backup kann binnen weniger Minuten Erfolgen. Die Dokumentation erfolgt im Ticket-System.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

a) Der ISO-27001 zertifizierte IT-Dienstleister des Verantwortlichen 1 hat ein umfassendes Datenschutz-Management-System implementiert, insbesondere eine Richtlinie zur DSGVO, Verarbeitungsverzeichnis, einen Datenschutzbeauftragten benannt, Schulung und Sensibilisierung der Mitarbeiter werden regelmäßig durchgeführt, usw.

b) Die bereitgestellte Software wurde konzipiert und programmiert, dass nur solche Daten verarbeitet werden, die für den Verarbeitungszweck (=Aufklärung von Compliance-Hinweisen) erforderlich sind. Bereits die Felder der Eingabemaske beschränken sich auf das absolut erforderliche Maß. Zudem besteht die Möglichkeit, den Meldern eine anonyme Abgabe der Meldung einzuräumen. Die Einstellungen der Plattform sind derart konzipiert, dass keine IP-Adressen oder sonstige Geräte-Daten getrackt werden, um die Vertraulichkeit/Anonymität der Hinweisgeber sicherzustellen. Die Hinweise werden zudem

Ende-zu-Ende verschlüsselt. Nur der Admin kann Manager zu einem Fall bzw. auf die Plattform einladen (mit 2-Faktor-Authentifizierung).

c) Der IT-Dienstleister des Verantwortlichen 1 evaluiert regelmäßig sein Datenschutz-Management-System und vergewissert sich regelmäßig von der datenschutzrechtlichen Zuverlässigkeit seiner Unterauftragnehmer und Lieferanten. Verantwortlicher 1 und dessen IT-Dienstleister haben jeweils einen Datenschutzbeauftragten bestellt. Die Datenschutzbeauftragten führen regelmäßige Begehungen durch, um die aktuellen Maßnahmen und Verfahren zu evaluieren sowie Optimierungen zu initiieren.

d) Verantwortlicher 1 arbeitet nur mit Subunternehmern zusammen, die hinreichend Garantien bieten (einschließlich ISO-27001 Zertifizierung), dass die Verarbeitung in Einklang mit den Vorschriften der DSGVO erfolgt. Mit den Subunternehmern werden Vereinbarungen zur Auftragsverarbeitung geschlossen.

e) Bei Einstellung werden die Mitarbeiter des IT-Dienstleisters auf Art. 28 Abs. 3 lit. b) DSGVO verpflichtet und bezüglich der Einhaltung des Datenschutzes am Arbeitsplatz über ein eigenes Datenschutzschulungstool geschult. Die Mitarbeiter des Verantwortlichen 1 unterliegen als Rechtsanwälte kraft ihres Berufsstandes einer strengen Verschwiegenheitspflicht aus § 43a Abs. 2 der Bundesrechtsanwaltsordnung (BRAO), wonach alle vertraulichen Informationen und personenbezogenen Daten, die im Rahmen der anwaltlichen Tätigkeit anvertraut werden, geschützt sind.