Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

der
GWA Hygiene GmbH

Stand
24.05.2018

„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 treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten …“ (Art. 32 DSGVO Abs. 1)

Die GWA Hygiene erfüllt diese Forderungen durch folgende Maßnahmen:

1. Organisatorisches

(Maßnahmen, die generelle Auswirkungen auf das Datenschutzniveau haben)

- Die Mitarbeiter werden mit Eintritt in das Beschäftigungsverhältnis über den Datenschutz aufgeklärt sowie auf das Datengeheimnis verpflichtet.
- Die Mitarbeiter werden durch regelmäßige Informationsrundschreiben, Belehrungen und Awareness-Maßnahmen über aktuelle datenschutzrechtliche Entwicklungen sowie besondere zu berücksichtigende Maßnahmen des Datenschutzes, bezogen auf das Unternehmen, informiert.
- Schulungen der Mitarbeiter werden nach Erforderlichkeit im Hinblick auf den jeweiligen Kenntnisstand und Aufgabenbereich der Mitarbeiter in regelmäßigen Abständen durchgeführt.

2. Vertraulichkeit (Art. 32 Abs. 1 DSGVO)

Zutrittskontrolle

(Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.)

- Die Unternehmensräumlichkeiten liegen in einem Bürokomplex, welcher Videoüberwacht ist und nachts zusätzlich von einem Sicherheitsdienst kontrolliert wird.
- Zutritt zu den Unternehmensräumlichkeiten erfolgt über den Haupteingang des Gebäudes sowie sodann separaten Bürozugang. Der Haupteingang kann zwischen 07:00 und 16:00 Uhr

frei passiert werden. Außerhalb dieses Zeitfensters ist der Eingang durch ein elektronisches Zutrittskontrollsystem geschützt.

- Der Eintrittsbereich wird von Mitarbeitern kontrolliert.
- Die Schlüsselvergabe an Mitarbeiter erfolgt mittels Schlüsselquittung (Protokollierung in Personalakte).
- Das operative Arbeiten erfolgt auf Servern, welche bei der Fa. Hetzner gehostet sind. Die Zutrittskontrolle zum Rechenzentrum der Fa. Hetzner wird wie folgt geregelt (Siehe auch https://www.hetzner.de/pdf/ADV_TOM.pdf):
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Hochsicherheitszaun um den gesamten Datacenterpark
    - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
    - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
    - 24/7 personelle Besetzung der Rechenzentren
    - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen

Zugangskontrolle

(Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.)

- Das Passwort zur Administrationsoberfläche der Server bei Fa. Hetzner wird von GWA Hygiene selbst vergeben. Server-Passwörter werden nach erstmaliger Inbetriebnahme von selbst geändert und sind der Fa. Hetzner nicht bekannt. Server-Passwörter sind nur ausgewählten Mitarbeitern mit entsprechendem Aufgaben- und Verantwortungsbereich zugänglich.
- Jeder Mitarbeiter verfügt über einen individuellen Login mit nur ihm bekannten individuellen Passwort (siehe auch „Zugriffskontrolle“).
- Jeder Mitarbeiter authentifiziert sich mittels 2 Faktor-Authentifizierung.
- Bei Pausen aktiviert sich nach einer bestimmten Zeit automatisch eine Bildschirmsperre.
- An- und Abmeldungen werden protokolliert.
- Verwendete Browser- und Antivirensoftware ist stets auf die neuste verfügbare Version aktualisiert.
- Es wird innerhalb des Betriebs ein verschlüsseltes W-LAN eingesetzt. Ein Empfang außerhalb des Bürogebäudes ist nicht möglich.

Zugriffskontrolle

(Maßnahmen, die geeignet sind, zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.)

- Für administrative Tätigkeiten (insbesondere Verwaltung von E-Mails, Dokumenten sowie die Nutzung von Kalenderfunktionen) wird auf Nextcloud zurückgegriffen.

- Der Anmeldeprozess eines Mitarbeiters lokal vor Ort erfordert zunächst eine Anmeldung an seinem Arbeitsplatzrechner mittels individuellem Login und Passwort.
- Der Mitarbeiter muss sich ferner beim Hygienemonitor anmelden. Nutzer werden hier durch die Administration entsprechend angelegt und freigeschaltet. Die Anmeldung des Mitarbeiters selbst erfolgt wiederum durch Login und Passwort.
- Beim Ausscheiden von Mitarbeitern werden deren Zugänge deaktiviert.
- Die Mitarbeiter haben nur Zugriff auf die für ihre Tätigkeit relevanten Daten. Es erfolgt eine differenzierte Berechtigungsvergabe. Beispielsweise ist bei Vertriebsmitarbeitern der Zugriff auf reine vertriebsrelevante Daten beschränkt.
- Sensible Systeme sind nur aus dem Intranet heraus zu erreichen.

Trennungskontrolle

(Maßnahmen, die geeignet sind, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.)

- Es erfolgt die logische Trennung der Kundendaten innerhalb des Datenbanksystems.
- Die interne Mandantenfähigkeit ist gewährleistet.
- Entwicklungs- und Produktivsysteme werden getrennt voneinander eingesetzt.

Pseudonymisierung

(Die Verarbeitung personenbezogener Daten soll, sofern erforderlich und umsetzbar, in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.)

- Die erfassten Betätigungen lassen keinen direkten Rückschluss auf den Menschen zu, der die Aktion durchführt. Jeder Betätigung wird einem oder keinem Transponder zugeordnet. Da die Transponder im Zufallsverfahren bei Schichtbeginn aus der Box entnommen werden ist die Zuordnung Transponder zu Person nicht möglich.

3. Integrität (Art. 32 Abs. 1 DSGVO)

Weitergabekontrolle

(Maßnahmen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.)

- Weitergaben physischer Datenträger erfolgen nicht. Mobile Datenträger werden nicht eingesetzt.
- Die Datenablage erfolgt auf dem Server und nicht lokal. Die Kommunikation zwischen Arbeitsplatzrechner und Server erfolgt über sichere verschlüsselte Datenübertragung.
- Alle Mitarbeiter sind auf die Einhaltung des Datengeheimnisses verpflichtet.
- Nach Auftragsbeendigung erfolgt die datenschutzgerechte Löschung der nicht mehr erforderlichen Daten.

- Sämtliche Festplatten in einem Arbeitsplatzrechner sind verschlüsselt.

Eingabekontrolle

(Maßnahmen, die geeignet sind, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.)

- An- und Abmeldungen werden systemintern protokolliert.
- Veränderungen können z.T. in der Datenbank eingesehen und nachgeprüft werden.

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 DSGVO)

Verfügbarkeitskontrolle

(Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

- In allen Büroräumen sind Brandmelder installiert. Es sind ausreichend und gewartete Feuerlöscher vorhanden und Fluchtwege gekennzeichnet.
- In den Büroräumlichkeiten herrscht Rauchverbot.
- Der Betrieb der Server bei der Fa. Hetzner erfolgt unter Einsatz unterbrechungsfreier Stromversorgung.
- Es besteht ein dauerhaft aktiver DDoS-Schutz.
- Virenschutzsoftware sowie eine Firewall werden eingesetzt. Regelmäßige Aktualisierungen gewährleisten die stete Aktualität.
- Es erfolgt die fortlaufende Spiegelung aller Daten auf Backup Server bei täglichen Backups aller Daten.

Rasche Wiederherstellbarkeit

Wiedereinspielungstests der Backups in regelmäßigen Abständen.

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

Datenschutz-Management

- Es wird ein internes Datenschutzkonzept vorgehalten mit Dokumentation zum Umgang mit personenbezogenen Daten. Die Überprüfung und Kontrolle erfolgt durch den Datenschutzbeauftragten.

Incident-Response-Management

- Im Rahmen des Notfallkonzepts als Bestandteil des Datenschutzkonzepts sind klare Prozesse zum Umgang mit IT-Sicherheitsvorfällen und Datenschutzvorfällen beschrieben.

Datenschutzfreundliche Voreinstellungen

- Für alle Entwicklungen wird dem Grundsatz Privacy-by-default bestmöglich gefolgt.

6. Auftragskontrolle

(Maßnahmen, die geeignet sind, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.)

- Beim verwendeten Hostingdienst (Hetzner) erfolgt die Anmietung der Netzwerkinfrastruktur, Bandbreite und Serverhardware. Die Installation und Wartung der Server erfolgen durch GWA Hygiene selbst.
- Zugangsdaten (Passwörter) der Server sind allein GWA Hygiene bekannt.

Inhaltlich verantwortlich:

Name: Maik Gronau
Funktion: Geschäftsführer
Telefon: 03831 20 355 47
E-Mail: maik.gonau@gwa-hygiene.de

Unterschrift