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

der
GWA Hygiene GmbH

Stand
13.09.2019

„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 GmbH erfüllt diese Forderungen durch folgende Maßnahmen:

# 1. Inhaltsverzeichnis

## 2. 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 und Belehrungen über aktuelle datenschutzrechtliche Entwicklungen sowie besondere zu berücksichtigenden 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.

# 3. Vertraulichkeit (Art. 32 Abs. 1 DSGVO)

## 3.1 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 über einen separaten Bürozugang. Der Haupteingang kann zwischen 07:00 und 18:00 Uhr frei passiert werden. Außerhalb dieses Zeitfensters ist der Eingang durch ein elektronisches Zutrittskontrollsystem bzw. durch einen Schlüssel geschützt.
- Zutritt zum Serverraum/IT-Infrastrukturraum nur durch Hausverwaltung möglich. (abgeschlossene Brandschutztür).
- Die Schlüsselvergabe an Mitarbeiter zu den entsprechenden Büroräumen, in denen die Mitarbeiter Zugang benötigten, um ihre Aufgabe zu erfüllen, 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.com/AV/TOM.pdf Stand: 10.09.2019):
    - 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

## 3.2 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. Anmeldung auf den Servern nur durch Public-Key-Authentifizierung möglich. Zugang zur Hetzner-Administrationsoberfläche wird über ein 2-Faktor-Authentifizierungsverfahren abgesichert (Sicherstellung der Authentizität).
- Jeder Mitarbeiter verfügt über einen individuellen Login mit nur ihm bekannten individuellen Passwort (siehe auch „Zugriffskontrolle“), um sich an einem beliebigen Arbeitsplatz in dem Bürogebäude oder an einem Laptop mit VPN-Tunnel anzumelden.

- Jeder Außendienstmitarbeiter benutzt einen VPN-Tunnel, um in das interne Netzwerk des Unternehmens zu gelangen. Dieser Tunnel benutzt die best-möglichste Verschlüsselung, die verwendbar ist (aktuell: AES-256-CBC).
- Bei Pausen oder Bildschirmarbeitsunterbrechungen wird die Bildschirmsperre von dem Mitarbeiter gesperrt. Sollte dies vergessen werden, wird diese automatisch nach 5 Minuten aktiviert.
- Computer- und Zugang-basierte An- und Abmeldungen werden protokolliert.
- Verwendete Browser- und Antivirensoftware werden regelmäßig auf die neuste verfügbare Version aktualisiert.
- Innerhalb des Betriebs werden abteilungsgetrennte verschlüsselte WLAN-Netzwerke eingesetzt. Der Empfang der Signale aus nächster Nähe zu dem Gebäude kann technisch bedingt nicht ausgeschlossen werden.

## 3.3 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. Die Kommunikation wird über HTTPS verschlüsselt.
- Der Anmeldeprozess eines Mitarbeiters lokal vor Ort erfordert zunächst eine Anmeldung an seinem Arbeitsplatzrechner mittels individuellem Login und Passwort.
- Der Mitarbeiter muss sich ferner über einen anderen Login an der firmeneigenen Software „Hygienemonitor“ (HM) anmelden. Nutzer werden hier durch die Administration entsprechend angelegt und freigeschaltet.
- Eine bereitgestellte Android-App zur Einrichtung des „Hygienemonitors“ durch den Servicetechniker (Service-App) kommuniziert mit HM stehts über einen HTTPS-verschlüsselten Tunnel. Diese zeigt zur Übersichtlichkeit für den Techniker die Kundennamen und deren Standorte an.
- 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.

## 3.4 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.

# 4. Integrität (Art. 32 Abs. 1 DSGVO)

## 4.1 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.)

- Mobile Datenträger können eingesetzt werden, wenn die Daten darauf mit einem sicheren Passwort[1] verschlüsselt werden und dieses Passwort über einen anderen Kanal mitgeteilt werden.
- 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.

## 4.2 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.)

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

[1] Richtlinie: min. ein Groß- und Kleinbuchstaben, ein Zahlen und Sonderzeichen und mindestens 12 Zeichen

# 5. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 DSGVO)

## 5.1 Verfügbarkeitskontrolle

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

- Es sind ausreichend und gewartete Feuerlöscher in den Fluren 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 Sicherung aller Daten auf Backup-Servern.

## 5.2 Rasche Wiederherstellbarkeit

- Wiedereinspielungstests der Backups in regelmäßigen Abständen.

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

## 6.1 Datenschutz-Management

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

## 6.2 Incident-Response-Management

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

## 6.3 Datenschutzfreundliche Voreinstellungen

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

## 7. 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 Serverdienstleister (Hetzner) erfolgt die Anmietung der Netzwerkinfrastruktur, Bandbreite und Serverhardware. Die Installation und Wartung der Server erfolgen durch GWA Hygiene GmbH selbst.
- Zugangsdaten (Public-Keys) der Server sind allein GWA Hygiene GmbH bekannt.

**Inhaltlich verantwortlich:**

**Name: Maik Gronau**
**Funktion: Geschäftsführer**
**Telefon: 03831 20 355 47**

**E-Mail: maik.gonau@gwa-hygiene.de**

Unterschrift