

# TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

# 1. Einleitung

## 1.1. Verantwortlicher

Verantwortlicher gem. Art. 4 Nr. 7 EU-Datenschutz-Grundverordnung (DSGVO) ist GWA Hygiene GmbH, Heinrich-Mann-Straße 11, 18435 Stralsund, Deutschland, E-Mail: [info@gwa-hygiene.de](mailto:info@gwa-hygiene.de). Gesetzlich vertreten werden wir durch Maik Gronau, Tobias Gebhardt.

## 1.2. Datenschutzbeauftragter

Unser Datenschutzbeauftragter ist die heyData GmbH, Kantstr. 99, 10627 Berlin, [www.heydata.eu](http://www.heydata.eu), E-Mail: [datenschutz@heydata.eu](mailto:datenschutz@heydata.eu).

## 1.3. Gegenstand des Dokuments

Dieses Dokument fasst die vom Verantwortlichen getroffenen technische und organisatorische Maßnahmen im Sinne von Art. 32 Abs. 1 DSGVO zusammen. Das sind Maßnahmen, mit denen der Verantwortliche personenbezogene Daten schützt. Das Dokument hat den Zweck, den Verantwortlichen bei der Erfüllung seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO zu unterstützen.

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

### 2.1. Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- Alarmanlage
- Chipkarten-/Transponder-Schließsystem
- Manuelles Schließsystem (z.B. Schlüssel)
- Sicherheitsschlösser
- Videoüberwachung der Zugänge
- Schlüsselregelung / Schlüsselbuch
- Besucher nur in Begleitung durch Mitarbeiter
- Arbeit im Home Office: Unbefugte haben kein Zutritt zur Wohnstätte der Mitarbeiter

## 2.2. Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben:

- Authentifikation mit Benutzer und Passwort
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Einsatz von VPN-Technologie bei Remote-Zugriffen
- Verwendung von Gehäuseverriegelungen
- Verschlüsselung von Datenträgern
- BIOS-Schutz (separates Passwort)
- Automatische Desktopsperre
- Verschlüsselung von Notebooks / Tablets
- Verwaltung von Benutzerberechtigungen
- Erstellen von Benutzerprofilen

- Zentrale Passwortregeln
- Nutzung von 2-Faktor-Authentifizierung
- Schlüsselregelung / Schlüsselbuch
- Allgemeine Anweisung, bei Verlassen des Arbeitsplatzes Desktop manuell zu sperren

## 2.3. Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

- Einsatz von Aktenvernichtern (mit cross cut-Funktion)
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Protokollierung von Zugriffen auf Anwendungen (insbesondere bei der Eingabe, Änderung und Löschung von Daten)
- Anzahl der Administratoren ist so klein wie möglich gehalten
- Sichere Aufbewahrung von Datenträgern
- Verwaltung der Benutzerrechte durch Systemadministratoren

## 2.4. Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Container Apps bei Nutzung privater Geräte für dienstliche Zwecke (BYOD)

## 3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

### 3.1. Weitergabekontrolle

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und

überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- Einrichtungen von VPN-Tunneln
- WLAN-Verschlüsselung (WPA2 mit starkem Passwort)
- Protokollierung von Zugriffen und Abrufen
- Bereitstellung von Daten über verschlüsselte Verbindungen wie SFTP oder HTTPS
- Uploadverbot dienstlicher Daten auf unternehmensfremde Server

## 3.2. Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Aufbewahrung von Formularen, deren Daten in automatisierte Verarbeitungen übernommen worden sind

- Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

- Feuer- und Rauchmeldeanlagen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Klimaanlage in Serverräumen
- Unterbrechungsfreie Stromversorgung (USV)
- RAID-System / Festplattenspiegelung



- Regelmäßige Backups
- Erstellung eines Backup- & Recoverykonzepts
- Kontrolle des Sicherungsvorgangs
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Keine sanitären Anlagen im oder oberhalb des Serverraums
- Trennung von Betriebssystemen und Daten
- Hosting (jedenfalls der wichtigsten Daten) mit einem professionellen Hoster

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

### **5.1. Datenschutz-Management**

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Verwendung der heyData-Plattform zum Datenschutz-Management
- Bestellung des Datenschutzbeauftragten heyData
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Regelmäßige Schulungen der Mitarbeiter im Datenschutz
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)

## 5.2. Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)
- Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls

## 5.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Die folgenden implementierten Maßnahmen tragen den Voraussetzungen der Prinzipien "Privacy by design" und "Privacy by default" Rechnung:

- Schulung der Mitarbeiter im "Privacy by design" und "Privacy by default"
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

## 5.4. Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

- Schriftliche Weisungen an den Auftragnehmer oder Weisungen in Textform (z.B. durch Auftragsverarbeitungsvertrag)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z.B. durch Anfrage entsprechender Bestätigungen
- Bestätigung von Auftragnehmern, dass sie ihre eigenen Mitarbeiter auf das Datengeheimnis verpflichten (typischerweise im Auftragsverarbeitungsvertrag)

- Sorgfältige Auswahl von Auftragnehmern (insbesondere hinsichtlich Datensicherheit)
- Laufende Überprüfung von Auftragnehmern und ihren Tätigkeiten
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z.B. durch Anfrage entsprechender Bestätigungen