

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

1. Einleitung

1.1. Verantwortlicher

Verantwortlicher gem. Art. 4 Nr. 7 EU-Datenschutz-Grundverordnung (DSGVO) ist Agentur Philipp GmbH, Mengkofener Straße 27, 84130 Dingolfing, Deutschland, E-Mail: info@agenturphilipp.de. Gesetzlich vertreten werden wir durch Philipp Mann.

1.2. Datenschutzbeauftragter

Unser Datenschutzbeauftragter ist die heyData GmbH, Schützenstraße 5, 10117 Berlin, www.heydata.eu, E-Mail: datenschutz@heydata.eu.

1.3. Gegenstand des Dokuments

Dieses Dokument fasst die vom Verantwortlichen getroffenen technischen und organisatorischen 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
- Absicherung von Gebäudeschächten
- Chipkarten-/Transponder-Schließsystem
- Manuelles Schließsystem (z.B. Schlüssel)
- Videoüberwachung der Zugänge
- Klingelanlage mit Kamera
- Besucher nur in Begleitung durch Mitarbeiter
- Sorgfältige Auswahl des Reinigungspersonals
- Anweisung an Mitarbeiter, nicht in öffentlich zugänglichen Räumlichkeiten (z.B. Cafés) zu arbeiten
- Arbeit im Home Office: Unbefugte haben kein Zutritt zur Wohnstätte der Mitarbeiter
- Arbeit im Home Office: Anweisung an Mitarbeiter, wenn möglich, in von Wohnräumen abgetrennten Arbeitszimmer zu arbeiten

2.2. Zugangskontrolle

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

- Authentifikation mit Benutzer und Passwort
- Authentifikation mit biometrischen Daten
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Einsatz von VPN-Technologie bei Remote-Zugriffen
- Sperren externer Schnittstellen (z.B. USB-Anschlüsse)
- Automatische Desktopsperre
- Verwaltung von Benutzerberechtigungen
- Nutzung von 2-Faktor-Authentifizierung
- Allgemeine Unternehmens-Richtlinie zum Datenschutz oder zur Sicherheit
- Unternehmens-Richtlinie für sichere Passwörter
- Unternehmens-Richtlinie "Löschen/Vernichten"
- Unternehmens-Richtlinie "Cleandesk"
- Unternehmens-Richtlinie zur Verwendung mobiler Geräte
- 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:

- Protokollierung von Zugriffen auf Anwendungen (insbesondere bei der Eingabe, Änderung und Löschung von Daten)
- Einsatz eines Berechtigungskonzepts
- Anzahl der Administratoren ist so klein wie möglich gehalten
- Sichere Aufbewahrung von Datenträgern
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Anweisung an Mitarbeiter, dass nur unbedingt erforderliche Daten ausgedruckt werden
- Anweisung an Mitarbeiter, dass Daten nur nach Rücksprache gelöscht werden

2.4. Trennungskontrolle

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

- Physisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Trennung von Produktiv- und Testsystem

- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Logische Mandantentrennung (softwareseitig)
- Bei pseudonymisierten Daten: Getrennte Aufbewahrung der Zuordnungsdatei auf einem getrennten, abgesicherten IT-System (möglichst verschlüsselt)
- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder nach Ablauf der gesetzlichen Löschfrist, wenn möglich, zu anonymisieren/pseudonymisieren.

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

- E-Mail-Verschlüsselung
- WLAN-Verschlüsselung (WPA2 mit starkem Passwort)
- Protokollierung von Zugriffen und Abrufen
- Bereitstellung von Daten über verschlüsselte Verbindungen wie SFTP oder HTTPS
- Nutzung von Signaturverfahren
- Sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Uploadverbot dienstlicher Daten auf unternehmensfremde Server
- Home Office: Fernlöschungsrecht des Arbeitgebers

3.2. Eingabekontrolle

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

- Manuelle oder automatische Kontrolle der Protokolle
- Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können

- 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
- Klare Zuständigkeiten für Löschungen
- Anweisung an Mitarbeiter, nur nach Rücksprache Daten zu löschen

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:

- Feuerlöschgeräte in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräume
- Unterbrechungsfreie Stromversorgung (USV)
- Datenschutztresor

- RAID-System / Festplattenspiegelung
- Videoüberwachung in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Regelmäßige Backups
- Erstellung eines Backup- & Recoverykonzepts
- Kontrolle des Sicherungsvorgangs
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Erstellen eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- 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