Technische & Organisatorische Maßnahmen (TOMs)

Im Folgenden werden die spezifischen technischen und organisatorischen Maßnahmen aufgelistet, die gemäß Art. 24(1) der EU-Datenschutz-Grundverordnung (DSGVO) für die Auftragsverarbeitung getroffen wurden.

Die heylogin GmbH erfüllt die in der DSGVO festgelegte Verpflichtung, die Verarbeitung von personenbezogenen Daten durch geeignete technische und organisatorische Maßnahmen zu schützen und, soweit möglich personenbezogene Daten zu anonymisieren oder zu pseudonymisieren. Alle getroffenen Maßnahmen müssen dabei das Risiko des jeweiligen Datenverarbeitungsvorgangs berücksichtigen und dem Stand der Technik entsprechen. Insbesondere sollte die Wirksamkeit der Maßnahme die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit berücksichtigen.

Definition der Schutzziele:

- **Vertraulichkeit**: Schutz von Daten, Informationen und Programmen vor unberechtigtem Zugriff.
- **Integrität**: Sachliche und technische Richtigkeit und Vollständigkeit aller Informationen und Daten bei der Verarbeitung.
- **Verfügbarkeit**: Informationen, Daten, Anwendungen, IT-Systeme und IT-Netze sind für die Verarbeitung erreichbar.
- **Belastbarkeit**: Bezeichnet einen Aspekt der Verfügbarkeit und damit die Fähigkeit von Informationen, Daten, Anwendungen, IT-Systemen und IT-Netzen im Falle von Störungen, Ausfällen oder starker Beanspruchung zu funktionieren.

1 Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen,die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Datenverarbeitet oder genutzt werden, zu verwehren.

Maßnahmen:

- Kein unbefugter Zutritt zu Datenverarbeitungsanlagen.
- Die Bürogebäude sind mit einer Schließanlage gesichert. Der Eingangsbereich wird videoüberwacht.
- Alle Datenverarbeitungsanlagen auf denen Kundendaten gespeichert werden befinden sich bei Unterauftragsverarbeitern.

1.2 Zugangskontrolle

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

Maßnahmen:

- Keine unbefugte Systembenutzung.
- Alle eigenen IT Anlagen sind mit sicheren Kennwörter gesichert.
- Beim Verlassen des Arbeitsplatzes wird der Desktop gesperrt.
- Das System erzwingt eine Mindestlänge von 16 Zeichen, wobei Zahlen und Buchstaben enthalten sein müssen.
- Die Rechtevergabe bei Neueintritt und Austritt von Mitarbeitern ist im Informationssicherheitsmanagementsystem geregelt.
- Die Anbieter von Hosting-Infrastruktur sind nach ISO 27001 zertifiziert.

1.3 Zugriffskontrolle

Maßnahmen, die 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.

Maßnahmen:

- Die Daten sind softwareseitig gegen unbefugtes Lesen, Kopieren, Verändern oder Entfernen gesichert.
- Logins werden protokolliert.
- Logins auf Produktivsystemen erzeugen Benachrichtigungen.
- Die Zugriffskontrollrichtlinie im Informationssicherheitsmanagementsystem definiert einen verbindlichen Prozess und Regeln für die Zugriffskontrolle auf interne und externe Systeme.

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Maßnahmen:

- Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.
- Das Produktivsystem ist mandantenfähig und stellt softwareseitig eine Trennung der Daten der einzelnen Kunden sicher.
- Jeder Kunde kann durch sein Login identifiziert nur auf die von ihm verwalteten Daten zugreifen.
- Das Produktivsystem ist strikt getrennt von Test- und Entwicklungssystemen.

1.5 Maßnahmen für mobiles Arbeiten / Homeoffice

Maßnahmen, die gewährleisten, dass die Verarbeitung personenbezogener Daten auch bei mobilem Arbeiten im Einklang mit den bestehenden Sicherheitsrichtlinien erfolgt und ein dem Büroarbeitsplatz gleichwertiges Schutzniveau gewährleistet ist.

Mobiles Arbeiten ist auf die im Auftragsverarbeitungsvertrag definierten Kundendaten beschränkt: Account-E-Mail-Adressen, Protokoll- und Metadaten sowie Support- und Gerätedaten. Alle anderen Daten (z. B. Nutzernamen, Passwörter) sind Ende-zu-Ende-verschlüsselt und technisch nicht durch Mitarbeitende auslesbar (vgl. Auftragsverarbeitungsvertrag 1.1).

Maßnahmen:

- Mobiles Arbeiten und Homeoffice-Arbeitsplätze unterliegen den entsprechenden Richtlinien im ISO-27001-zertifizierten Informationssicherheitsmanagementsystem. Alle Mitarbeitenden sind vertraglich zur Einhaltung verpflichtet.
- Alle Endgeräte sind mit vollständiger Festplattenverschlüsselung oder einem gleichwertigen Mechanismus geschützt und werden regelmäßig mit den neuesten Sicherheitsupdates und Patches versorgt.
- Der Zugriff auf Endgeräte ist nur mit lokalen Benutzerkonten möglich, die durch Passwörter gemäß der Passwort-Richtlinie geschützt sind.
- Alle Endgeräte werden gemäß bestehender Richtlinien gesperrt, sobald sich die Benutzer von ihrem Arbeitsplatz entfernen.
- Arbeitsplätze sind gemäß bestehender Richtlinien frei von ungesicherten sensiblen Informationen, Unterlagen, Schränke, Schubladen und Bildschirme sind stets gesichert.

2 Gewährleistung der Integrität

2.1 Weitergabekontrolle

Maßnahmen, die 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.

Maßnahmen:

- Alle Datenübertragungen zwischen heylogin und externen Systemen finden ausschließlich über verschlüsselte Verbindungen statt. Das verwendete Protokoll ist TLS in Version 1.2 oder höher.
- Daten in Papierform werden mit einem Aktenvernichter nach ISO/IEC 21964 mit der Vernichtungsstufe P4 datenschutzgerecht entsorgt. Elektronische Datenträger werden gesammelt und nach ISO/IEC 21964 mit den Vernichtungsstufen E4, H4 entsorgt.

2.2 Eingabekontrolle

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

Maßnahmen:

- Die Datenverarbeitung erfolgt direkt durch den Kunden.

3 Pseudonymisierung und Verschlüsselung

3.1 Pseudonymisierung

Maßnahmen, die eine Pseudonymisierung von Daten gewährleisten.

Maßnahmen:

- Personenbezogene Daten werden zur längerfristigen Speicherung nach 30 Tagen pseudonymisiert. Die Pseudonymisierung erfolgt durch Vergabe von UUID-Bezeichner.

3.2 Verschlüsselung

Maßnahmen, die eine Verschlüsselung von Daten gewährleisten.

Maßnahmen:

- Die Nutzung von Verschlüsselungsverfahren erfolgt nach aktuellem Stand der Technik.

- Daten werden bei der elektronischen Übertragung oder während ihres Transports verschlüsselt übertragen. Das verwendete Protokoll ist TLS in Version 1.2 oder höher.
- Inhaltliche Kundendaten werden ausschließlich Ende-zu-Ende-verschlüsselt gespeichert. Die verwendeten Verfahren sind XSalsa20+Poly1305 sowie X25519.
- Backups inhaltlicher Kundendaten werden zusätzlich verschlüsselt. Das verwendete Tool ist „age“.

4 Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

4.1 Verfügbarkeit (der Daten)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Verfügbarkeit von Daten.

Maßnahmen:

- Alle Kundendaten werden stündlich auf mindestens einem externen System gesichert.
- Die Systeme der eingesetzten Unterauftragsverarbeiter sind per USV gegen Stromausfall gesichert.
- Eine Firewall schützt den Zugriff von außen auf alle Systeme.
- Alle Produktivsysteme sind geo-redundant ausgelegt, so dass bei einem Ausfall einer Komponente eine andere Komponente die Aufgaben sofort übernehmen kann.

4.2 Belastbarkeit (der Systeme)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Belastbarkeit der Systeme.

Maßnahmen:

- Monitoring der Produktiv-Systeme.
- Alerting bei unerwarteten Abweichungen im Monitoring.

4.3 Wiederherstellbarkeit (der Daten / der Systeme)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Wiederherstellbarkeit von Daten und Systemen.

Maßnahmen:

- Vollständige Wiederherstellung des Betriebes aus einem aktuellen Backup innerhalb von ca. zwei Stunden.

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen:

- Abschluss der notwendigen Auftragsdatenvereinbarungen.
- Abschluss der notwendigen Standard-Vertragsklauseln.
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten.
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis.
- Sicherstellung der Vernichtung von Daten nach Beendigung eines Auftrags.

5.2 Datenschutz-Management

Maßnahmen, die gewährleisten, dass Methoden evaluiert wurden, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, organisieren, steuern und kontrollieren.

Maßnahmen:

- Regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen nach dem PDCA-Zyklus (Plan-Do-Check-Act).
- Einhaltung der Informationspflichten gemäß Art. 13 DSGVO.
- Einhaltung der Informationspflichten gemäß Art. 14 DSGVO.
- Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz.
- Durchführung von Datenschutzfolgeabschätzungen (bei Bedarf).
- Regelmäßige Sensibilisierung der Mitarbeiter zum Datenschutz.
- Überprüfung der Wirksamkeit der TOMs (mind. jährlich durchgeführt).
- Verpflichtung der Mitarbeiter auf das Datengeheimnis.

5.3 Incident-Response-Management

Maßnahmen, die gewährleisten, dass Sicherheitsvorfällen vorgebeugt werden kann oder im Falle von bereits eingetretenen Sicherheitsvorfällen, dass Daten und Systeme geschützt werden können und eine schnelle Analyse und Behebung des Sicherheitsvorfalls durchgeführt werden kann.

Maßnahmen:

- Dokumentation von Sicherheitsvorfällen.
- Einsatz von Firewall und deren regelmäßige Aktualisierung.
- Einsatz von Spamfilter und deren regelmäßige Aktualisierung.
- Einsatz von Virenscanner und deren regelmäßige Aktualisierung.
- Einsatz von kontinuierlichen Schwachstellen-Scans der Codebase und Infrastruktur.

5.4 Datenschutzfreundliche Voreinstellungen

Maßnahmen, die gewährleisten, dass bereits durch die entsprechende Technikgestaltung (privacy by design) und Werkseinstellungen (privacy by default) einer Software vorab ein gewisses Datenschutzniveau herrscht.

Maßnahmen:

- Personenbezogene Daten werden nur zweckerforderlich erhoben.