Anhang A4

Technical and Organisational Measures

1 Maßnahmen zur Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle

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

Allgemeines (dokumentiertes) Gebäudesicherungskonzept
Schließsystem/ Schließanlage (mit Sicherheitsschlössern)
Alarmanlage
Videoüberwachung der Eingänge
(konkretes) Zutrittsberechtigungskonzept
Begleitung von Besuchern durch Mitarbeiter
Elektronische Zutrittscodekarten/ Zutrittstransponder
Schlüsselregelung (u.a. Schlüsselverzeichnis; separate Schließung einzelner Büros)
Sorgfältige Auswahl von Reinigungspersonal

1.2 Zugangskontrolle

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

Rollenkonzept
Berechtigungsmanagement
Erstellen von Benutzerprofilen
Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen
Dokumentierter Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
Verwendung von individuellen Passwörtern
Login mit Benutzername und Passwort
Login mit biometrischen Daten
Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)
Richtlinie „sicheres Passwort“(mit Mindestvorgaben zur Passwortkomplexität):
• Mindestens 8 Zeichen

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Wien
hello@heylog.com;

• Mindestens 8 Zeichen für lokale Admin-Passwörter
• Groß- und Kleinschreibung, Sonderzeichen, Zahl (davon mind. 3 Kriterien)
Zeitverzögerung zwischen einzelnen Login-Versuchen
Fehlgeschlagene Anmeldeversuche werden Nutzern angezeigt
Zwei- oder Mehrfaktorauthentifizierung bei Verarbeitungen mit hohem Risiko
Speichern v. Passwörtern im Browser nur mit Masterpasswort
Verschlüsselung von Notebooks / Tablets
Verschlüsselung von Netzwerken
• Verwendete Verschlüsselungsalgorithmen: WPA3
Verhinderung der Ausführung von heruntergeladener Software, deren Quellen als unsicher gekennzeichnet werden
Nutzung von VPN-Technologie
Einsatz einer Software-Firewall
Standard-Authentifizierungsinformationen werden nach Softwareinstallation/erstem Login geändert
Regelung zum Home Office / zu Telearbeit

1.3 Zugriffskontrolle

Maßnahmen, die sicherstellen, dass zur Nutzung eines Datenverarbeitungssystems berechtigte Personen nur auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten während der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Verwaltung der Benutzerrechte durch Administratoren
Nutzung eines Berechtigungskonzepts
Minimaler Einsatz von Administratoren-Konten (Mindestanzahl von Administratoren)
Verschiedene administrative Rollen nach least Privilege-Konzept (Benutzer, Firewall, Backups etc.)
Superuser (z.B. root unter Linux) soweit möglich nicht verwendet
Regelmäßige Überprüfung von Rollen und Berechtigungen
Regelmäßige Auswertung von Protokollen (Logfiles)
Zeitliche Begrenzung von Zugriffsmöglichkeiten
Protokollierung von Dateizugriffen
Protokollierung von Dateilöschungen
Protokollierung von Dateiveränderungen
SPAM-Filter
Verschlüsselte Speicherung der Daten
Verwendete Verschlüsselungsalgorithmen: AES (128/256 bit)

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Wien
hello@heylog.com;

Verwendete Hash-Funktion: SHA3
Zwei-Faktor-Authentifizierung zur Wartung von Webservern
SSL Zertifikate nur aus vertrauenswürdigen Stellen
Einsatz von WLAN nur auf aktuellen Routern mit wirksamen Zugangsmechanismen
WLAN-Gastzugang ohne Zugriff auf internes Netzwerk
Prüfung eingehender E-Mails mittels Anti-Malware

2 Maßnahmen zur Gewährleistung der Integrität

2.1 Weitergabekontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten während der elektronischen Übermittlung oder während des Transports oder der Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Datenübertragungseinrichtungen übermittelt werden sollen.

Wie werden Daten zwischen dem Verantwortlichem und Dritten übermittelt?
• VPN-Verbindung
E-Mail-Verschlüsselung (SMIME)
Protokollierung von Zugriffen und Abrufen
Bereitstellung über verschlüsselte Verbindungen wie sftp, https
Datenaustausch über https-Verbindung (verwendetes Verschlüsselungsprotokoll: TLS 1.3)
Bei HTTPS: Einsatz von Client-Zertifikaten
Regelung zur Nutzung von Cloud-Diensten (inkl. Exit-Strategie)

2.2 Eingabekontrolle

Maßnahmen, die sicherstellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, geändert oder aus ihnen entfernt wurden. Die Kontrolle kann durch die Nutzung der Protokollierungsfunktionalitäten erfolgen

Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
Manuelle oder automatisierte Auswertung der Protokolle
Differenzierte Benutzerberechtigungen:
• Einzelne Benutzernamen, keine Benutzergruppen
• Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
Verpflichtung auf das Datengeheimnis
Nachvollziehbarkeit der Dateneingabe, -änderung und -löschung durch individuelle Benutzernamen (nicht Benutzergruppen)

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Wien
hello@heylog.com;

Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf der Grundlage eines Berechtigungskonzepts. Der Benutzer kann keine Daten in der Anwendung löschen oder ändern, er kann eine Anfrage an GDPR@heylog.com senden und die Daten werden innerhalb von 48h angepasst.

3 Maßnahmen zur Gewährleistung der Verfügbarkeit & Belastbarkeit

3.1 Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Brandmeldeanlagen in Serverräumen
Rauchmelder in Serverräumen
Brandschutztüren
Wasserlose Brandbekämpfungssysteme in Serverräumen
Wassersensoren in Serverräumen
Blitz-/ Überspannungsschutz
Klimatisierte Serverräume
Serverräumlichkeiten in separaten Brandabschnitt
Unterbringung von Backupsystemen in separaten Räumlichkeiten und in separatem Brandabschnitt
Serverräume nicht unter oder neben sanitären Anlagen
Zutrittsbegrenzung bei Serverräumen auf notwendiges Personal
Alarmmeldung bei unberechtigtem Zutritt zu Serverräumen
CO2-Feuerlöscher in unmittelbarer Nähe der Serverräume
USV-Anlage (Unterbrechungsfreie Stromversorgung)
Stromgenerator
Dokumentiertes Datensicherungs- und Backupkonzept
Regelmäßige Tests zur Datenwiederherstellung
Gewährleistung der langfristigen technischen Lesbarkeit von Backupspeichermedien
Regelmäßige Datenwiederherstellungstests und Protokollierung der Ergebnisse: Die Wiederherstellungstests werden jedes letzte Quartal des Jahres durchgeführt.
Die Kontrolle des Backup-Prozesses erfolgt täglich durch den Admin der Google Cloud, bei fehlgeschlagenen Backups wird eine Benachrichtigung verschickt.
Backup & Recovery-Konzept (formuliert): Heylog macht ein nächtliches Backup und wird von AWS verwaltet.

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Wien
hello@heylog.com;

3.2 Belastbarkeit (Widerstandsfähigkeit und Ausfallkontrolle)

Soll Systeme befähigen, mit risikobedingten Veränderungen umgehen zu können und Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufzuweisen.

Redundante Stromversorgung
Redundante Datenanbindung
Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)
Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates
Regelmäßige Sensibilisierung der Mitarbeiter (mind. jährlich)
Abschluss einer Cyber-Versicherung

4 Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Kontrollverfahren

Maßnahmen, die die Wirksamkeit der Datensicherheitsmaßnahmen gewährleisten.

Verarbeitungsverzeichnisse (Art. 30 I und II DSGVO) werden jährlich aktualisiert
Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert
Regelmäßige Überprüfung und Auswertung der eingesetzten Software
Prüfung der Wirksamkeit getroffener Sicherheitsmaßnahmen mind. jährlich
Bei Feststellungen im Rahmen der zuvor gen. Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst
Prozess zur Reaktion auf Sicherheitsverletzungen (Angriffe) und Systemstörungen existiert (Incident-Response-Management)
Dokumentation von Sicherheitsvorfällen
Einsatz von Security Intelligence (Real Time-Analyse; log management, SIEMs, NBADs, network forensics)

4.2 Auftragskontrolle

Soll sicherstellen, dass Daten, die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftraggebers verarbeitet werden.

Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO) *sofern möglich*
Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)
Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer

4.3 Trennungskontrolle

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Wien
hello@heylog.com;

Maßnahmen, die sicherstellen, dass für unterschiedliche Zwecke erhobene Daten getrennt verarbeitet werden können.

Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)
Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)
Trennung von Entwicklungs-, Test- und Produktivsystem https://app-dev.heylog.com : **Entwicklungsumgebung** https://staging.heylog.com/ : **Testumgebung** https://app.heylog.com/ : **Live-Umgebung**
Festlegung von Datenbankrechten
Steuerung über Berechtigungskonzept

4.4 Datenschutzmaßnahmen für das Heylog System und dessen Entwicklung

Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenverletzungen (auch im Hinblick auf die Meldepflicht an die Aufsichtsbehörde).
Dokumentation von Sicherheitsvorfällen und Datenschutzverletzungen wird an gdpr@heylog.com gesendet.
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.
Einfache Ausübung des Widerrufsrechts der betroffenen Person durch manuelle Maßnahmen der Organisation.
Mindestens einmal jährlich ist eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen durchzuführen.
Regelmäßige Sensibilisierung der Mitarbeiter

4.5 Sonstiges Datenschutz- bzw. Sicherheitsmanagement

Geeignete Organisationsstruktur für Informationssicherheit mit eindeutig festgelegten Rollen
Einsatz einer Datenschutzmanagement-Software
zentrale Dokumentation aller Verfahren und Regelungen zum Datenschutz
Geschulte und auf Vertraulichkeit / Datengeheimnis verpflichtete Mitarbeiter
Allgemeine Datenschutz- und Sicherheitsrichtlinie
Dokumentierter Prozess zum Umgang mit IT-Sicherheitsvorfällen
Klare Verantwortlichkeiten bei der Handhabung von Datenschutz- und Sicherheitsvorfällen
Dokumentierter Prozess zur Sicherstellung von Betroffenenrechten
zentrale, für alle Mitarbeiter zugängliche Ablage von Richtlinien/ Prozessen/ Verfahrensanweisungen

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Wien
hello@heylog.com;

Externe Dienstleister werden, soweit nötig, zur Verschwiegenheit verpflichtet
Regelmäßige Schulungen zu den Richtlinien und Sicherheitsprozessen
Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer, sofern eine Verpflichtung zur Bestellung besteht.

Heylog FlexCo; Icon Tower 24/3 - Regus; Wiedner Gürtel 13; 1100 Wien
hello@heylog.com;