Technische und organisatorische Maßnahmen im Sinne des Datenschutzes

Technische und organisatorische Maßnahmen

Die Gedys Intraware GmbH als Anbieter von CRM-Software und zugehörigen Services hat eine Vielzahl technischer und organisatorischer Maßnahmen implementiert, um die vom Auftraggeber übermittelten Daten zu schützen. Diese Maßnahmen sind darauf ausgelegt, den Anforderungen des Datenschutzes und der Datensicherheit gerecht zu werden und gewährleisten insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Die festgelegten Sicherheitsvorkehrungen werden kontinuierlich überwacht und gepflegt, um einen hohen Standard im Bereich des Datenschutzes zu gewährleisten. Dabei wird stets berücksichtigt, dass detaillierte Informationen zu spezifischen Sicherheitsmaßnahmen aus Gründen des Schutzes vor unbefugtem Zugriff und zur Vermeidung von Sicherheitslücken nicht in vollem Umfang offengelegt werden können. Dies ist besonders im Kontext von Datenschutz und Datensicherheit erforderlich, da der Schutz dieser Maßnahmen gegen unbefugte Offenlegung mindestens ebenso wichtig ist wie die Sicherheitsmaßnahmen selbst.

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

Zutrittskontrolle

Die Zutrittskontrolle dient dem physischen Schutz von Datenverarbeitungsanlagen, die personenbezogene Daten verarbeiten, indem sie unbefugtem Zugang wirksam vorbeugt. Der Begriff „Zutritt“ bezieht sich dabei auf den räumlichen Zugang zu den betroffenen Anlagen.

- Sicherheitsschlösser
- Zutrittsberechtigungskonzept
- Manuelles Schließsystem
- Schließsystem mit Codesperre
- Schlüsselregelung / Schlüsselbuch
- Chipkarten-/Transponder-Schließsystem
- Rechenzentren mit Standort in Deutschland oder der EU
- separate Serverräume
- Sorgfältige Auswahl von Reinigungspersonal

Zugangskontrolle

Die Zugangskontrolle stellt sicher, dass das Eindringen Unbefugter in DV-Systeme sowie deren unbefugte Nutzung verhindert wird, indem nur autorisierte Personen Zugang zu den Systemen erhalten.

- Getrenntes Gäste-WLAN
- Detaillierte Benutzerprofile
- Authentifikation mit Benutzer + Passwort
- Passwortregelungen
  - Verwendung von individuellen Passwörtern
  - Passwörter mit einer Mindestlänge
  - Anzahl von aufeinanderfolgenden Fehlversuchen ist begrenzt
  - Passworthistorie
- Schlüsselregelung
- Verschlüsselung von mobilen Datenträgern
- Autonome Fernwartung
- Zugriff nur per VPN auf internem Server
- Zentrale Änderung der Zugangsberechtigungen durch IT-Verantwortliche
- Protokollierung der Serverzugriffe auf Benutzerebene

Gedys Intraware GmbH | Eigilstr. 2 | D-36043 Fulda
P +49 661 9642 0 | info@gedys-intraware.de | gedys.com

Technische und organisatorische Maßnahmen im Sinne des Datenschutzes

Zugriffskontrolle

Die Zugriffskontrolle sorgt dafür, dass nur befugte Nutzer auf EDV-Systeme zugreifen können und dieser Zugriff auf die für ihre Aufgaben notwendigen Daten beschränkt ist. Unerlaubte Tätigkeiten außerhalb der eingeräumten Berechtigungen werden effektiv verhindert.

- Detailliertes Berechtigungskonzepts
- Sichere Aufbewahrung von Datenträgern
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduzieren
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Einsatz von Dienstleistern zur Akten- und Datenvernichtung (i.d.R. Möglichkeit mit Zertifikat)
- Einsatz von Intrusion-Detection-Systemen
- Einsatz von VPN-Technologie
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall
- Einsatz von Anti-Viren-Software

Trennungskontrolle

Die Trennungskontrolle stellt sicher, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt verarbeitet werden.

- Festlegung von Datenbankrechten
- Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt
- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)

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

Weitergabekontrolle

Die Weitergabekontrolle gewährleistet, dass personenbezogene Daten während der Übertragung, des Transports oder der Speicherung auf Datenträgern vor unbefugtem Zugriff, Veränderung, Kopieren oder Löschung geschützt sind. Aspekte der Weitergabe personenbezogener Daten sind zu regeln.

- Elektronische Übertragung, Datentransport, sowie deren Kontrolle.
- Einsatz von verschlüsselten Verbindungen (z.B. VPN, TLS)
- Sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- Shredder für die sichere Vernichtung von Daten
- Datenschutzboxen für die Entsorgung von vertraulichen Papierdokumenten

Eingabekontrolle

Die Eingabekontrolle stellt sicher, dass nachvollzogen werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder gelöscht wurden. Die Dokumentation und Nachvollziehbarkeit der Datenverwaltung und -pflege sind zu gewährleisten.

- Protokollierung der Eingabe, Änderung und Löschung von Daten

- Folgende Aktivitäten werden protokolliert: Hoch- und Herunterfahren von zentralen Rechnern (v.a. Servern und Firewalls)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

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

Verfügbarkeitskontrolle und Belastbarkeit

Die Verfügbarkeitskontrolle stellt sicher, dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind. Systeme müssen in der Lage sein, mit risikobedingten Veränderungen umzugehen und eine hohe Toleranz sowie Ausgleichsfähigkeit gegenüber Störungen aufzuweisen.

- Feuerlöschgeräte in Serverräumen
- Testen von Datenwiederherstellung
- Schutzsteckdosenleisten in Serverräumen
- Serverräume nicht unter sanitären Anlagen
- Backup- & Recoverykonzept
- Unterbrechungsfreie Stromversorgung (USV)
- Aufbewahrung von Datensicherung an einem sicheren, separaten Ort
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen / IT-Räumen

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

Kontrollverfahren

Im Rahmen der Kontrollverfahren gewährleistet der Auftragnehmer, dass personenbezogene Daten nur gemäß den Weisungen des Auftraggebers verarbeitet werden. Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren.

- Unternehmensrichtlinien (Code of Conduct) vorhanden
- Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzkoordinator und -beauftragten
- Datenschutz-Management vorhanden
- Datenschutz-Konzept vorhanden

Technische und Organisatorische Maßnahmen beim mobilen Arbeiten

Die Gedys Intraware ermöglicht ihren Mitarbeitenden, anfallende Arbeiten via Remote-Zugang durchzuführen. Hierfür wurden Maßnahmen ergriffen, um dem Sicherheitsstandard des allgemeinen Sicherheitskonzeptes zu entsprechen. Dieses gilt, soweit anwendbar und wird um die folgenden Maßnahmen ergänzt.

Die Maßnahmen unterteilen sich in **technische Maßnahmen**, die den Zugang zum System betreffen sowie in **organisatorische Maßnahmen**, die den Umgang des jeweiligen Mitarbeiters mit Daten an seinem Heimarbeitsplatz betreffen.

Technische Maßnahmen

Die nachfolgenden Maßnahmen stellen die zusätzlich ergriffenen Maßnahmen dar. Für den Zugriff auf das System hat Gedys Intraware/ Proalpha folgende Maßnahmen getroffen:

Technische und organisatorische Maßnahmen im Sinne des Datenschutzes

- Zugang ausschließlich über dienstliche Endgeräte
- Endgeräte werden IT-seitig regelmäßigen Updates unterzogen
- Applikationen dürfen ausschließlich nach Konsultation der hierfür vorliegenden Whitelist installiert werden. IT-seitig nicht zugelassene Applikationen dürfen nicht installiert werden.
- Ein Zugriff erfolgt ausschließlich durch eine verschlüsselte VPN-Verbindung
- Windows Clients
  - Endpoint Security
  - Antivirus Software
  - Systemverschlüsselung
- iOS Clients
  - verwaltet durch Intune Mobile Device Management (MDM)
    - Kontrolle über das Gerät mit Möglichkeit zum remote „wipe“ bzw. „lock“
  - komplette Verschlüsselung des Gerätes
  - geschützt durch sechsstelligen Pass Code
  - restriction policy
    - nicht vertrauenswürdige Zertifikate können nicht manuell akzeptiert werden
    - keine Diagnosedaten an Apple
    - Benutzer kann keinen 3rd-Party Apps manuell vertrauen

Organisatorische Maßnahmen

In organisatorischer Hinsicht wurden in Ergänzung zu den Maßnahmen der allgemeinen TOM verschiedene Zusatzvereinbarungen sowie interne Richtlinien erlassen. Dies umfasst unter anderem Folgende Regelungen und Verpflichtungen:

- Zutritts- und Kontrollrecht des Arbeitsplatzes durch interne beauftragte Prüfer (z.B. Fachkraft für Arbeitssicherheit oder betrieblicher Datenschutzkoordinator/ -beauftragter)
- Verpflichtung auf interne Richtlinie zur Nutzung technischer Einrichtungen
- Verpflichtung zum Schutz des Zugriffs unbefugter Dritter auf Arbeitsmittel
- Untersagung der Verwendung eigener technischer Einrichtungen (Ausgenommen WLAN, Peripheriegeräten wie Tastatur und Maus ohne Treiberinstallation)
- Verpflichtung, vertrauliche dienstliche Dokumente unter Verschluss zu halten (Cleandesk)
- Verpflichtung auf Vertraulichkeit / zur Geheimhaltung
- Verpflichtung, Wohnortswechsel mitzuteilen