Anlage 1
Technische und Organisatorische Maßnahmen gem. Art. 32 DSGVO der mySolution Software & Consulting GmbH

1. Vertraulichkeit

a. Zutrittskontrolle

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

- Unbefugten und insbesondere betriebsfremden Personen ist der Zugang grundsätzlich verwehrt; er kann erst nach ausdrücklicher Freigabe durch einen Mitarbeiter unter Benennung des Anlasses ermöglicht werden.
- Es existieren sowohl Sicherheitsschlösser wie auch eine Schlüsselregelung.
- Server sind in abgeschlossenen Räumen oder Schränken untergebracht.
- Datensicherungen auf portable Sicherungsmedien (z.B. CD/DVD, Bänder) sind in zutritts-geschützten Räumen untergebracht.

b. Zugangskontrolle

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

- Der Zugang zur technischen Arbeitsumgebung ist durch Benutzername und Passwort geschützt.
- Es existiert eine Passwort-Richtlinie. In diesem Zusammenhang wird eine gewisse Pass-wortlänge- und Komplexität gefordert sowie das Benutzerkonto nach einer vorgegebenen Anzahl von Falschanmeldungen gesperrt.
- Nicht mehr benötigte Zugangsberechtigungen werden zeitnah entzogen.
- Der Arbeitsplatzrechner wird nach einer vorgegebenen Zeitdauer der Inaktivität gesperrt.
- Es werden Logs der Benutzeranmeldungen erstellt.
- Die Arbeitsplatzrechner sind durch Anti-Viren-Software geschützt.
- Das Reinigungspersonal wird sorgfältig ausgesucht.

c. 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.

- Es sind ausschließlich Personen, die mit der Erhebung, Nutzung und Verarbeitung der Daten im Rahmen der vereinbarten Auftragsverarbeitung betraut sind, berechtigt, die Daten zu lesen, zu kopieren, zu ändern oder zu löschen. In diesem Zusammenhang bestehen klare Regelungen zur Vergabe von Zugriffsberechtigungen, die einen differenzierten Zugriff (lesen, ändern, löschen) berücksichtigen und den Zugriff auf den verschiedenen Ebenen regeln.
- Für eventuelle Fernadministration sind Sicherheitsregeln in Kraft.
- Papierunterlagen können beim Verlassen des Arbeitsplatzes vor unbefugter Kenntnisnahme bzw. unbefugtem Zugriff durch die Möglichkeit abschließbarer Schränke bzw. Fächer geschützt werden.
- Es existieren folgende technische Sicherheitseinrichtungen zum Schutz gegen einen Zugriff aus nicht vertrauenswürdigen Netzwerken (z.B. Internet): Firewall
- Die technischen Sicherheitseinrichtungen werden regelmäßig auf ihre Wirksamkeit hin geprüft.

d. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Im Hinblick auf personenbezogene Daten verschiedener Auftraggeber erfolgt eine logische Trennung der Daten (Mandantenprinzip).
- Es erfolgt ferner eine physikalische Unterscheidung zwischen Produktiv- und Testsystem.

2. Integrität

a. 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.

- Die Verwendung von externen Datenträgern (USB-Stick, externe Festplatte, CDs, DVDs) außerhalb der geschützten Unternehmensumgebung ist nur im verschlüsselten Zustand erlaubt.
- Die datenschutzgerechte Datenvernichtung ist gewährleistet. Bei Papierdokumenten erfolgt sie durch einen Papierreißwolf. Bei Datenträgern (z.B. defekte Festplatte) erfolgt sie physikalisch.
- Der Datenkanal mit dem Auftraggeber ist verschlüsselt.
- Zusätzlich sind die Daten verschlüsselt.

b. 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.

- Um zu gewähren, dass im Nachhinein geprüft werden kann, ob, von wem und wann personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, erfolgt eine entsprechende softwareseitige Protokollierung.

3. Verfügbarkeit und Belastbarkeit

a. Verfügbarkeitskontrolle

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

- Sofern vertraglich vereinbart sind die Daten gegen zufällige Zerstörung oder Verlust geschützt.
- Es gibt ein Backup- und Recoverykonzept.
- Die Backups werden regelmäßig daraufhin getestet, ob ein reibungsloses Zurücksichern möglich ist.

b. Unverzügliche Wiederherstellbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei einem physischen oder technischen Zwischenfall unverzüglich wiederhergestellt werden können.

- Es existiert ein Konzept für die Wiederherstellung des Geschäftsbetriebs nach einem Notfall.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a. Datenschutz-Management

- Es ist ein Datenschutz- und Sicherheitskonzept vorhanden, das regelmäßig überprüft wird.
- Das Datenschutz- und Sicherheitskonzept wird an sich ändernde Bedingungen angepasst.

b. Incident Response-Management

- Es gibt eine Prozessbeschreibung zur Behandlung von Datenpannen.
- Die Mitarbeiter sind über den Ablauf der Behandlung von Datenpannen informiert.

c. Auftragskontrolle

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

- Aus der Leistungsbeschreibung, die als Grundlage der Auftragsverarbeitung zwischen Auftragnehmer und Auftraggeber vereinbart wurde, gehen Art, Umfang und Zweck der Datenverarbeitung klar hervor.
- Die mit der Umsetzung der Auftragsverarbeitung befassten Mitarbeiter sind über den Leistungsumfang informiert.
- Für die vereinbarte Auftragsverarbeitung werden ggf. Cloud-Lösungen eingesetzt. Die genutzten Rechenzentren befinden sich in der EU. Die Cloud-Datenkommunikation ist verschlüsselt.