

Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage

Vertraulichkeit

Zugangskontrolle Server:

- Zugang zu den IT technischen Systemen bei der Podstawski Group Deutschland haben nur vom Geschäftsführer benannte Personen. Zugang wird durch individuelle Anmeldungen gewährt, Daten durch entsprechende Gruppenberechtigungen getrennt und der Zugriff darüber geregelt
- Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
- Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung
- Zugang ist passwortgeschützt, Zugriff besteht nur für berechnigte Mitarbeiter vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert
- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden
- Für übertragene Daten/Software ist einzig der Auftraggeber in Bezug auf Sicherheit und Updates zuständig

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle:

- Alle bei der Podstawski Group beschäftigten Mitarbeiter und Dienstleister die mit IT technischen Systemen in Kontakt kommen, sind i.S.d. Art 32 Abs.4 DSGVO verpflichtet und unterwiesen den datenschutzkonformen Umgang mit personenbezogenen Daten umzugehen
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung
- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt

Eingabekontrolle

- Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
- Änderungen der Daten werden protokolliert.
- Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- bei internen Verwaltungssystemen des Auftragnehmers
- Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
- Sachkundiger Einsatz von Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
- Einsatz von Festplattenspiegelung bei allen relevanten Servern.
- Monitoring aller relevanten Server.
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Datensicherung obliegt dem Auftraggeber

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

- Die Interne IT Struktur wird durch tägliche Datensicherungen auf externe Medien gesichert – eine vollständige Wiederherstellung ist somit tagesweise möglich

Auftragskontrolle

- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.