

Technisch und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten.

*Maßnahmen zur fortdauernden Sicherstellung der **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung:*

Vertraulichkeit

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen (mehrstufige Schließanlage mit Schlüssel), elektrische Türöffner, Videoanlage, Aktenschränke mit Schloss

Zugangskontrolle: Schutz vor unbefugter Systembenutzung (Kennwörter, einschließlich entsprechender Policy), Zwei-Faktor-Authentifizierung (Google Authenticator)

Zugriffskontrolle: Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems nur nach Freigabe; Standardprozess für Berechtigungsvergabe und -entzug; Protokollierung von Änderungen (erstellen, ändern und löschen von Dateien); administrative Benutzerkonten auf das absolute Minimum beschränkt.

Integrität

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, wenn vollständig innerhalb der Google-Cloud abgewickelt.

Eingabekontrolle: Personenbezogene Daten des Kunden/Auftraggebers werden nur von diesem in die Systeme (zB Google Analytics) übernommen (Event-Log, Protokollierung).

Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen:

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust (Google-Cloud-Lösung), Virenschutz; Sicherungskonzept innerhalb der Google Cloud Services; Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern; rasche Wiederherstellbarkeit.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung:

Datenschutz-Policy, einschließlich regelmäßiger **Mitarbeiter-Schulungen**.

Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Kunden, durch eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO- und andere Zertifizierungen), laufende und anlassbezogene Kontrollen.

Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden:

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen (mehrstufige Schließanlage mit Schlüssel), elektrische Türöffner, Videoanlage, Aktenschränke mit Schloss

Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

Löschfristen:

- Zugangsdaten und Berechtigungen von Mitarbeiterinnen und Mitarbeitern werden in einem standardisierten Prozess nach dem Ausscheiden entzogen.
- Personenbezogene Daten von Betroffenen des Auftraggebers werden nach schriftlicher Aufforderung bzw 12 Monate nach Beendigung jeglicher Vertragsverhältnisse zwischen Auftraggeber und e-dialog gelöscht, sofern dem keine gesetzlichen Aufbewahrungspflichten entgegenstehen.
- Kontaktdaten des Auftraggebers unterliegen einer gesetzlichen Aufbewahrungsfrist (Rechnungslegung, Dokumentation, ...) und werden nach deren Ablauf gelöscht.

Die genehmigten Unterauftragsverarbeitern (e-dialog GmbH und e-dialog AG) treffen als Teil der e-dialog Gruppe genau die gleichen technischen und organisatorischen Maßnahmen.