

Vereinbarung zur Auftragsdatenverarbeitung (gemäß Art. 28 DSGVO)

webgo GmbH

Wandsbeker Zollstr. 95
22041 Hamburg
Deutschland

T · 040 605 900 399
F · 040 605 900 398

info@webgo.de
[webgo.de](https://www.webgo.de)

Anlage 2: Technische und Organisatorische Maßnahmen

§1 Vertraulichkeit

§1.1 Zutrittskontrolle

Zutrittskontrollsystem, Chipkarte, Türsicherung (elektrische Türöffner, Gegensprechanlage), Videoüberwachung des Geländes, Vermeidung von Datenverarbeitungen im Erdgeschoss, Überwachung und Begleitung von Dienstleistern und Besuchern und zugehörige Stichprobenkontrollen

§1.2 Zugangskontrolle

Schriftliche Fixierung der Zugangsberechtigungen, restriktive Vergabe von Zugangsberechtigungen, Einrichtung und Pflege einer elektronischen Benutzerverwaltung, Ausgestaltung der Passwörter möglichst nach Vorgaben des BSI (u. a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts), Erstellung einer Passworrichtlinie in Form einer Dienstanweisung, automatische Sperrung (z. B. Kennwort, Pausenschaltung oder bei mehrfachen Fehlversuchen der Nutzung), Verwendung von Firewalls/Antivirensoftware

§1.3 Zugriffskontrolle

Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte), Protokollierung und Auswertung der Zugriffe und Zugriffsversuche, technische Einschränkung der Abfrage- und Zugriffsmöglichkeiten, Regelung der Datenlöschung bzw. Datenträgervernichtung, Verwendung von Magnet- oder Chipkarten/biometrischen Verfahren zur Authentifikation

§1.4 Trennungskontrolle

"Interne Mandantenfähigkeit" (Kunden- bzw. Mandantentrennung), Dokumentation von Zwecken, zu denen die Daten erhoben wurden, Vergabe unterschiedlicher Rollen in Systemen, Trennung von Test- und Produktivdaten

§1.5 Pseudonymisierung

Erstellung und Aktualisierung einer Übersicht über die ergriffenen technischen und organisatorischen Maßnahmen, Abschluss eines schriftlichen Vertrags zur Auftragsverarbeitung mit den gesetzlichen Mindestinhalten sowie darüber hinausgehenden Informationen zur genauen Auftragsgestaltung, Zugänglichmachung des Vertrags zur Auftragsverarbeitung und der Weisungen für die involvierten Beschäftigten, Schulung der Mitarbeiter auf die Anforderungen an den Datenschutz in Auftragsverarbeitungsverhältnissen, Verpflichtung der Beschäftigten auf Einhaltung des Datenschutzes, Verschlüsselung von Daten während der Übermittlung, Trennung der Daten

§1.6 Datenschutzfreundliche Voreinstellungen

Alle personenbezogenen Daten werden nur für den vorgegebenen Zweck verarbeitet.

§2 Integrität

§2.1 Weitergabekontrolle

Aufzeichnung und Dokumentation aller durchgeführten und geplanten Übermittlungen mit Nennung des Empfängers, der Datenkategorien, des Übermittlungszwecks, des Absenders und des Datums sowie der Uhrzeit der Übermittlung, Erlass von Arbeitsanweisungen bzw. Richtlinien zur Datenträgernutzung und Datenübermittlung, Führen einer Übersicht der wiederkehrenden bzw. regelmäßigen Übermittlungen und deren Ablauf, Nutzung eines VPN, Nutzung eines Content-Filters/einer Firewall, Verbot der Mitnahme oder des Mitbringens von privaten Datenträgern, datensichere Entsorgung von Daten und Datenträgern, Nutzung sicherer Transportfahrzeuge, Nutzung von Übertragungsprotokollen wie TLS/SSL oder SSH

§2.2 Eingabekontrolle

Protokollierungs- und Protokollauswertungssysteme, Erlass von Dienstanweisungen und Schulung zur Eingabe/Veränderung/Entfernung von personenbezogenen Daten sowie deren Zulässigkeit, Protokollierung der Benutzeranmeldungen an Datenverarbeitungsanlagen, Protokollierung von erfolgreichen und gescheiterten Software-Log-ins, Protokollierung der Aktivitäten auf Servern und der Systemverwalter sowie Benutzer

§2.3 Verfügbarkeit und Belastbarkeit

Back-up-Verfahren, Spiegeln von Festplatten (RAID), unterbrechungsfreie Stromversorgung (USV), Installierung von Schutzsteckdosenleisten, Brandschutztüren, Alarmanlagen, Blitzableiter, Bereitstellung von Feuerlöschern, Installierung von Brandmeldern, Durchführung von Brandschutzbegehungen, Installierung von Brandfrüherkennungsanlagen

§2.4 Organisatorische Maßnahmen

Regelmäßige Mitarbeiterschulungen mit Nachweis, schriftlich unterschriebene Verpflichtung auf das Datengeheimnis, schriftliche Arbeitsanweisungen, Dokumentation von Auskunftersuchen, Anliegen, Berichtigungen, Löschungen oder Sperrungen von personenbezogenen Daten, Verpflichtung aller Dienstleister auf den Datenschutz, IT-Sicherheitsbeauftragten, etablierte Meldeprozesse für Datenschutzverstöße und Incident-Response-Management für IT-Sicherheitsvorfälle

§2.5 Kontrollen der technischen und organisatorischen Maßnahmen

Anlassbezogene Kontrollen, Sichtung und Auswertung von Protokoll- und Logdateien, Sichtung von manuellen Protokollen und Listen, Prüfungen durch den Datenschutzbeauftragten




webgo GmbH
Wandsbeker Zollstr. 95, 22041 Hamburg
Tel.: +49 (0) 4103 900-100
info@webgo.de - www.webgo.de

Hamburg, 14.05.2018

Ort, Datum

Auftragnehmer