

# A1 Business Secure Gate

## Datenschutzanhang

Version: 1.0

Vom: 20.01.2025

## 1. Datenschutzanhang

Im Rahmen der Erbringung des A1 Business Secure Gate-Services agiert A1 Digital Deutschland GmbH als Auftragsverarbeiter (AV) für die personenbezogenen Daten der Kunden.

Produktname	Sub-Auftragsverarbeiter (je nach Wahl der Lösung und wie im Angebot definiert)	Land der Verarbeitung
<b>A1 Business Secure Gate</b>	<b>A1 Telekom Austria AG</b> <b>Zscaler Inc.</b>	<b>Österreich</b> <b>EU</b>

*Tabelle 1: Auftragsverarbeiter*

### Welche Daten werden erhoben?

- ☒ **Personen-Stammdaten**
- ☐ **Personen-Kennungen**
- ☐ **Besondere personenbezogene Daten**
- ☐ **Marketing/Sales-Daten mit Personenbezug**
- ☒ **Personen-Rollen/-Assoziationen**
- ☒ **Kundeninventar**
- ☒ **Kundeninteraktionen**
- ☐ **Dokumente**
- ☒ **Verkehrsdaten (z.B.: IP Adressen, Netzwerk Aktivitäten, Event Logs)**
- ☒ **Bewegungsdaten | Geolocation Data**
- ☒ **Inhaltsdaten (z.B.: Log Daten)**
- ☐ **Finanzdaten**
- ☒ **Login, Passwörter**

### Wer sind die Betroffenen?

- ☒ **Vertragspartner Kunde nat. Person**
- ☒ **Vertragspartner Kunde jur. Person**
- ☒ **Vertragspartner Kunde berechtigter Mitarbeiter**
- ☐ **User Enterprise Kunde**
- ☐ **Nicht A1 Kunde**
- ☐ **sonstiger Ansprechpartner des Vertragspartners**
- ☐ **Kinder**

- ☐ **Schutzbedürftige Personen (krank / behindert)**
- ☒ **A1 Mitarbeiter (Leasing und Fixangestellte)**
- ☐ **Vertragspartner Lieferanten**
- ☐ **Vertragspartner Lieferanten Mitarbeiter**

### **Technisch-organisatorische Maßnahmen**

Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen zur Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Sofern in der Leistungsvereinbarung nicht genauer geregelt, obliegt es dem Auftragsverarbeiter, dass der jeweiligen Verarbeitung angemessene Schutzniveau insbesondere durch eine Kombination der nachstehend genannten technisch organisatorischen Maßnahmen sicherzustellen. Es ist dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

#### **1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

##### **Zutrittskontrolle**

- Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pfortner, Alarmanlagen, Videoanlagen;

##### **Zugangskontrolle**

- Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen,
- Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

##### **Zugriffskontrolle**

- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.:
- Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

##### **Trennungskontrolle**

- Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden,
- z.B. Mandantenfähigkeit, Sandboxing;

##### **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)**

- Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

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

Weitergabekontrolle

- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

Eingabekontrolle

- Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

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

Verfügbarkeitskontrolle

- Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/off-line; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

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

## **4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)**

Datenschutz-Management;

Incident-Response-Management;

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);