persodesk

Datenschutzerklärung (B2B) für persodesk

Digital Bridges GmbH
Dahlmannstraße 1
37073 Göttingen

Version: 1.0
Stand: 9. März 2026

Inhaltsverzeichnis

Version: 1.0

§ 1 Geltungsbereich und Abgrenzung

Diese Datenschutzerklärung gilt für die Verarbeitung personenbezogener Daten im Rahmen der B2B-Hauptplattform von persodesk.

Sie gilt insbesondere für:

- Ansprechpartnerinnen und Ansprechpartner von Unternehmenskunden,
- Administratorinnen und Administratoren im Kundenkonto,
- von Unternehmenskunden angelegte oder eingeladene Mitarbeitende,
- Personen, die über einen Self-Onboarding-Link Daten in die Plattform eingeben.

Nicht von dieser Erklärung erfasst sind:

- das B2C-Vergleichs- und Wechselportal,
- das separate Versicherer-Portal.

Für diese Bereiche gelten jeweils eigenständige Datenschutzerklärungen.

§ 2 Verantwortliche Stelle und Rollenmodell

Soweit in dieser Datenschutzerklärung nichts Abweichendes beschrieben ist, ist Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO:

Digital Bridges GmbH
Dahlmannstraße 1
37073 Göttingen
E-Mail: datenschutz@digital-bridges.de

Rollenabgrenzung

Je nach Verarbeitungssituation handeln wir datenschutzrechtlich in unterschiedlichen Rollen:

1. Als Verantwortliche, wenn wir Daten für eigene Zwecke verarbeiten, insbesondere für:
   - Verwaltung von Vertrags-, Kontakt- und Kontobeziehungen mit Unternehmenskunden,
   - technische Konto-, Authentifizierungs-, Session- und Berechtigungsverwaltung,
   - Betriebssicherheit, Fehleranalyse sowie Missbrauchs- und Betrugsprävention,
   - Admin-, Audit- und Sicherheitsprotokolle sowie technische Zugriffsdaten,
   - Onboarding-Token, signierte Links und vergleichbare technische Zugriffssicherungen,
   - Bearbeitung von Supportanfragen, Supportfall-Metadaten und Kommunikationsverläufen,
   - Abrechnung, Compliance, Rechtsverteidigung und Durchsetzung vertraglicher Ansprüche.
2. Als Auftragsverarbeiterin für Unternehmenskunden, wenn wir Daten ausschließlich nach dokumentierter Weisung des jeweiligen Unternehmenskunden verarbeiten. Dies betrifft regelmäßig kundengesteuerte Inhalts-, Prozess-, Integrations- und Upload-Daten innerhalb der Plattform. In diesen Fällen gilt ergänzend der Auftragsverarbeitungsvertrag (AVV) mit dem jeweiligen Kunden. Soweit im Supportfall ein Zugriff auf solche Daten erforderlich ist, erfolgt dieser nur zur Bearbeitung des konkreten dokumentierten Vorgangs.

§ 3 Datenschutzkontakt

Kontakt für Datenschutzanfragen:

- E-Mail: datenschutz@digital-bridges.de

- Post: Digital Bridges GmbH, Dahlmannstraße 1, 37073 Göttingen

§ 4 Kategorien personenbezogener Daten

Je nach Nutzung werden insbesondere folgende Datenkategorien verarbeitet:

1. Stammdaten
    - z. B. Name, Vorname, dienstliche Kontaktdaten, Arbeitgeberzuordnung, Rolleninformationen.
2. Kontodaten und Berechtigungsdaten
    - z. B. Login-Informationen, Passwort-Hash, Rollen, Zugriffsrechte, Mandantenzuordnung.
3. Nutzungs- und Protokolldaten
    - z. B. Zeitpunkte von Zugriffen, Ereignisprotokolle, IP-Adresse (ggf. gekürzt), Browser- und Geräteinformationen.
4. Fachdaten im Plattformkontext
    - z. B. Angaben zu Beschäftigungsverhältnissen, versicherungsbezogene Angaben, Prozess- und Statusinformationen.
5. Kommunikationsdaten
    - z. B. Inhalte und Metadaten von Supportanfragen, E-Mails, Tickets.
6. Einwilligungsdaten
    - z. B. Nachweise zu Einwilligungen, soweit solche im Einzelfall für zusätzliche optionale Verarbeitungen außerhalb des Standardbetriebs eingeholt werden.

Je nach Verarbeitungskontext verarbeiten wir diese Daten entweder in eigener Verantwortlichkeit oder als Auftragsverarbeiterin. Kundengesteuerte Fachdaten im Plattformkontext fallen regelmäßig in den Verantwortungsbereich des jeweiligen Unternehmenskunden; Login-, Session-, Sicherheits-, Missbrauchs-, Token- und Supportfall-Metadaten verarbeiten wir typischerweise in eigener Verantwortlichkeit.

Nach aktuellem Produktstand ist die reguläre Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO nicht vorgesehen. Solche Daten sollen nicht in die Plattform eingestellt oder übermittelt werden. Gehen sie gleichwohl ein, verarbeiten wir sie nur in dem Umfang, der technisch für Prüfung, Absicherung, Sperrung, Support und Löschung erforderlich ist.

§ 5 Zwecke und Rechtsgrundlagen der Verarbeitung

Im Folgenden beschreiben wir die wesentlichen Verarbeitungen im B2B-Bereich:

5.1 Einrichtung und Verwaltung von Kundenkonten

Zwecke

- Anlage und Verwaltung von Organisationen, Nutzerrollen und Berechtigungen.

Rechtsgrundlagen

- Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung),
- Art. 6 Abs. 1 lit. f DSGVO (Sicherstellung eines geordneten und sicheren Plattformbetriebs).

5.2 Verarbeitung im Rahmen von Fachprozessen der Kundinnen und Kunden

Zwecke

- Verarbeitung von durch Kundinnen/Kunden bereitgestellten Daten zur technischen Bereitstellung der Plattformfunktionen.

Rechtsgrundlagen und Rolle

- Verarbeitung erfolgt typischerweise weisungsgebunden als Auftragsverarbeiterin gemäß Art. 28 DSGVO auf Basis des AVV.
- Die primäre Rechtsgrundlage gegenüber den betroffenen Personen liegt in der Verantwortung der jeweiligen Kundin/des jeweiligen Kunden.

5.3 Self-Onboarding von Mitarbeitenden

Zwecke

- Bereitstellung und Betrieb von Einladungs- und Onboarding-Strecken,
- Identitäts- und Vollständigkeitsprüfung von eingegebenen Daten,
- Übergabe an das jeweilige Kundenkonto.

Rechtsgrundlagen und Rolle

- Die inhaltliche Verarbeitung der im Self-Onboarding eingegebenen Daten erfolgt regelmäßig weisungsgebunden als Auftragsverarbeiterin für die einladende Organisation auf Grundlage von Art. 28 DSGVO.
- Die primären Rechtsgrundlagen gegenüber den betroffenen Personen liegen bei der einladenden Organisation.
- Eigene Verarbeitungen der Anbieterin beschränken sich auf technisch erforderliche Authentifizierungs-, Session-, Token-, Sicherheits-, Missbrauchs- und Protokollierungszwecke auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO.

5.4 Betriebssicherheit, Fehleranalyse und Missbrauchsprävention

Zwecke

- Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit,
- Erkennung und Abwehr unberechtigter Zugriffe und missbräuchlicher Nutzung.

Rechtsgrundlagen

- Art. 6 Abs. 1 lit. c DSGVO (gesetzliche Pflichten zur IT-Sicherheit, soweit einschlägig),
- Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an einem sicheren Plattformbetrieb).

5.5 Support und Kommunikation

Zwecke

- Bearbeitung von Anfragen,
- Fehlerbehebung,
- vertragsbezogene Kommunikation mit Ansprechpartnerinnen und Ansprechpartnern des Kunden.

Rechtsgrundlagen

- Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung),
- Art. 6 Abs. 1 lit. f DSGVO (effiziente Bearbeitung und Qualitätssicherung).

Support-Ticket-Metadaten, Kommunikationsverläufe und interne Bearbeitungshinweise verarbeiten wir regelmäßig in eigener Verantwortlichkeit zur Organisation, Qualitätssicherung und Rechtsverteidigung.

Soweit Supportzugriffe auf vom Kunden gesteuerte Fachdaten erforderlich sind, erfolgen diese als Auftragsverarbeiterin ausschließlich zur Bearbeitung des konkreten dokumentierten Supportfalls und auf Basis dokumentierter Weisungen, Freigaben oder vertraglich vorgesehener Supportabläufe.

§ 6 Empfängerinnen und Empfänger / Auftragsverarbeitung

Personenbezogene Daten werden nur weitergegeben, wenn hierfür eine Rechtsgrundlage besteht. Empfänger können insbesondere sein:

1. Technische Dienstleister
   - Hosting, Infrastruktur, Wartung, Monitoring, Kommunikationsdienste.
2. Weitere Auftragsverarbeiter
   - nur auf vertraglicher Grundlage gemäß Art. 28 DSGVO.
3. Behörden und öffentliche Stellen
   - soweit eine gesetzliche Verpflichtung besteht (Art. 6 Abs. 1 lit. c DSGVO).
4. Beraterinnen/Berater und Prüfer
   - soweit zur Rechtsverfolgung, Compliance oder Prüfung erforderlich (Art. 6 Abs. 1 lit. f DSGVO).

Eine Weitergabe zu anderen Zwecken erfolgt nur mit gesonderter Rechtsgrundlage oder Einwilligung.

§ 7 Drittlandübermittlungen

Eine Übermittlung in Staaten außerhalb des Europäischen Wirtschaftsraums (EWR) erfolgt nur, wenn die gesetzlichen Voraussetzungen erfüllt sind.

Als geeignete Garantien kommen insbesondere in Betracht:

- Angemessenheitsbeschlüsse der Europäischen Kommission,
- Standardvertragsklauseln (SCC),
- ergänzende technische und organisatorische Schutzmaßnahmen.

Informationen zu konkreten Übermittlungen stellen wir auf Anfrage bereit, soweit rechtlich zulässig.

§ 8 Speicherdauer und Löschung

Wir speichern personenbezogene Daten nur so lange, wie es für die jeweiligen Zwecke erforderlich ist.

Typische Speicherdauern (Orientierung):

- Authentifizierungs-, Session- und technische Zugriffsdaten: bis zum Ende der Sitzung oder für eine längere Wiedererkennung in der Regel bis zu `7 Tage`; serverseitige Sitzungsdaten in der Regel bis zu `24 Stunden`.
- Protokoll- und Sicherheitsdaten: in der Regel `7 bis 90 Tage`, abhängig vom Sicherheitszweck.
- Supportfall-Metadaten und Kommunikationsdaten: in der Regel `12 Monate` nach Abschluss des Vorgangs.
- Vertrags- und abrechnungsrelevante Daten: entsprechend gesetzlicher Aufbewahrungspflichten (regelmäßig `6 oder 10 Jahre`).
- Self-Onboarding-Daten ohne Abschluss: Löschung oder Anonymisierung nach Ablauf definierter Inaktivitätsfristen (z. B. `30 bis 180 Tage`).

Bei Sicherheitsvorfällen, Missbrauchsverdacht, offenen Rechtsansprüchen, Betroffenenbeschwerden, behördlichen oder gerichtlichen Verfahren sowie dokumentierten Legal Holds können relevante Daten bis zur Klärung und darüber hinaus bis zum Ablauf einschlägiger Aufbewahrungs- oder Verjährungsfristen gespeichert werden.

Sobald der Zweck entfällt und keine gesetzliche Aufbewahrungspflicht besteht, werden Daten ge-

löscht oder anonymisiert.

Soweit wir Daten als Auftragsverarbeiterin verarbeiten, richten sich Rückgabe und Löschung im Übrigen nach den Weisungen des jeweiligen Unternehmenskunden, dem AVV und dem dort geregelten Löschkonzept.

§ 9 Pflicht zur Bereitstellung von Daten

Bestimmte personenbezogene Daten sind erforderlich, damit wir das B2B-Portal bereitstellen und vertragliche Leistungen erfüllen können.

Werden erforderliche Daten nicht bereitgestellt, kann die Nutzung einzelner Funktionen oder des gesamten Portals eingeschränkt oder unmöglich sein.

§ 10 Rechte betroffener Personen

Betroffene Personen haben im Rahmen der gesetzlichen Voraussetzungen insbesondere folgende Rechte:

- Auskunft (Art. 15 DSGVO),
- Berichtigung (Art. 16 DSGVO),
- Löschung (Art. 17 DSGVO),
- Einschränkung der Verarbeitung (Art. 18 DSGVO),
- Datenübertragbarkeit (Art. 20 DSGVO),
- Widerspruch (Art. 21 DSGVO),
- Widerruf erteilter Einwilligungen mit Wirkung für die Zukunft (Art. 7 Abs. 3 DSGVO).

Zur Ausübung dieser Rechte genügt eine formlose Mitteilung an: `datenschutz@digital-bridges.de`

Sofern wir Daten als Auftragsverarbeiterin verarbeiten, leiten wir Anfragen unverzüglich an die jeweilige Kundin/den jeweiligen Kunden als primär Verantwortliche(n) weiter.

§ 11 Beschwerderecht bei einer Aufsichtsbehörde

Betroffene Personen haben das Recht, sich bei einer Datenschutzaufsichtsbehörde zu beschweren (Art. 77 DSGVO), insbesondere im Mitgliedstaat ihres gewöhnlichen Aufenthalts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes.

Für Digital Bridges GmbH kann insbesondere zuständig sein: Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5, 30159 Hannover
E-Mail: poststelle@lfd.niedersachsen.de

§ 12 Datensicherheit

Wir treffen angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Dazu gehören insbesondere Maßnahmen zur:

- Zugangskontrolle,
- Zugriffskontrolle,
- Weitergabekontrolle,
- Eingabekontrolle,
- Verfügbarkeitskontrolle,
- Trennung von Datenbeständen.

§ 13 Keine automatisierten Einzelentscheidungen

Es erfolgt keine ausschließlich automatisierte Entscheidung im Sinne von Art. 22 DSGVO mit rechtlicher oder ähnlich erheblicher Wirkung, sofern in produktbezogenen Dokumentationen nicht ausdrücklich etwas anderes beschrieben ist.

§ 14 Änderungen dieser Datenschutzerklärung

Wir passen diese Datenschutzerklärung an, wenn sich Verarbeitungen, rechtliche Anforderungen oder technische Rahmenbedingungen ändern.

Die jeweils aktuelle Fassung wird in der Plattform und/oder unter den rechtlichen Hinweisen zu persodesk veröffentlicht.