

Datenschutz – enmeshed Wallet

enmeshed ist eine datenschutzfreundliche Kommunikations- und Walletlösung, die in hochsensiblen Bereichen wie öffentlicher Verwaltung, Gesundheit, Bildung und Versicherungen eingesetzt wird. Das System entspricht dem höchsten Stand der Technik und ermöglicht Ende-zu-Ende-verschlüsselte, bidirektionale und DSGVO-konforme Datenflüsse zwischen natürlichen und juristischen Personen.

Ihr Ansprechpartner



Thomas Steinmetz
Chief Technology Officer
thomas.steinmetz@js-soft.com
+49 6221 43121-21

Unsere Datenschutz-Grundsätze

Datenminimierung

Es werden nur die nötigsten Daten erhoben, verarbeitet und gespeichert.

Löschkonzept

Daten werden auf Wunsch umgehend oder nach frei definierbarer Inaktivitätszeit gelöscht.

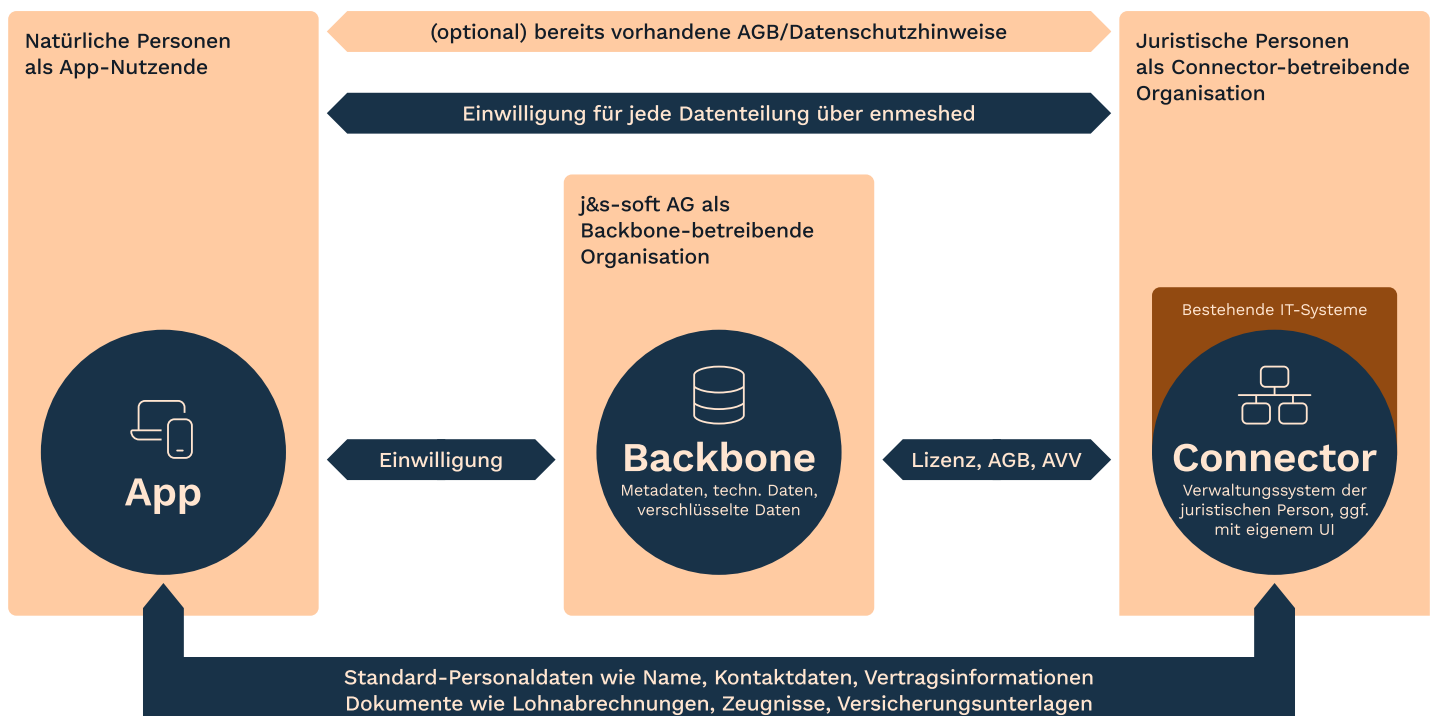
Einwilligungspflicht

Ohne explizite Einwilligung erfolgt keine Datenverarbeitung.

Technische Sicherheit

Alle Daten sind zu jedem Zeitpunkt bestmöglich nach aktuellem Stand der Technik geschützt.

Übersicht Datenflows und Einwilligungen



Sicherer zentraler Betrieb

- **Backbone-Verarbeitung:** Es werden ausschließlich Chiffren, Pseudonyme und indirekte personenbezogene Daten nach Art. 5 Abs. 1 lit. c DSGVO (Datenminimierung) gespeichert. Eine zentrale Datenlöschung ist möglich und kann mit einer Löschfrist nach Art. 17 DSGVO individuell festgelegt werden.
- **Betriebsort:** Der Backbone wird vollständig in der EU und durch EU-Bürger:innen betrieben und administriert, sodass Art. 44 ff. DSGVO (Keine Übermittlungen in Drittländer) eingehalten wird.
- **Hosting:** Dies erfolgt ausschließlich in zertifizierten Rechenzentren innerhalb der EU (ISO 27001 und C5 Zertifikat).
- **Metadatenfilter:** Es werden keine Tracking-Daten wie IP-Adressen, Gerätetypen oder Browserinformationen nach Art. 25 DSGVO gespeichert
- **Auftragsverarbeiter:** Die j&s-soft AG agiert als Auftragsverarbeiter nach Art. 28 DSGVO für den Backbone-Betrieb und ggf. als Unterauftragnehmer im App-Betrieb.

Datenschutz für Natürliche und Juristische Personen

Für Natürliche Personen

- **Nutzerfreundlichkeit:** Datenschutz ist essenziell, aber nicht störend – die App bleibt intuitiv.
- **Zentrale Anlaufstelle:** Für Datenschutzanfragen steht ein Supportteam zur Verfügung.
- **Transparenz & Kontrolle:** Nutzer:innen können einzelne Attribute, Kontakte und Profile nach Art. 5 Abs. 1 lit. e (Speicherbegrenzung), Art. 16 (Berichtigung) und Art. 17 (Löschung) DSGVO löschen und verändern:
 - **Attribut oder Kontakt:** Es erfolgt die sofortige Entfernung in der App. Löszeitpunkt und -umfang in den Systemen der Connector-betreibenden Organisation richtet sich nach deren Datenschutzbestimmungen.
 - **Profil:** Nach Beantragung wird dieses für 14 Tage deaktiviert. Innerhalb dieser Frist kann die Löschung widerrufen werden. Nach Ablauf erfolgt die wendgültige und unwiderrufliche Entfernung aller personenbezogenen Daten.

Für Juristische Personen

- **Rechtsgrundlage:** Die Nutzung basiert auf Freiwilligkeit und informierter Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO.
- **Eigene Datenschutzhinweise:** Können eingebunden und bei Kontaktaufnahme mit Nutzenden nach Art. 13 und 14 DSGVO (Informationspflichten) angezeigt werden.
- **Automatisierung:** Viele Datenschutzprozesse lassen sich vollständig digital abbilden z.B. Auskunft, Widerruf, Löschung aber auch alle weiteren Betroffenenrechte nach Art. 12-22 DSGVO.
- **Automatische Löschung:** Viele Daten können mit einem Ablaufdatum versehen werden. Nach Ablauf werden diese automatisch nach Art. 5 Abs. 1 lit. e DSGVO (Speicherbegrenzung) gelöscht.
- **Vertragliche Regelung:** Ein Auftragsverarbeitungsvertrag (AVV) mit der j&s-soft AG ist erforderlich.

Datenbezug und geprüfte Sicherheit

- **Unterstützung von absolutem Datenbezug** für behördliche Kunden, sodass verschlüsselte Daten als personenbezogen behandelt werden und **relativem Datenbezug** für Unternehmenskunden, um Datenschutzprozesse gemäß DSGVO pragmatischer zu gestalten.
- **Open-Source-Kern** für Transparenz, Nachvollziehbarkeit und externe Evaluation.
- **Sicherheitsprüfungen** mit Sicherheitsberater:innen durch interne und externe Audits finden regelmäßig statt.

Nächste Schritte für Datenschutzbeauftragte

