Data Processing Agreement Working Draft

Stand: 2026-06-08

Status: Arbeitsentwurf, keine Rechtsberatung. Vor externer Verwendung juristisch pruefen lassen.

Dieses Dokument ist eine fachliche Vorlage fuer einen Auftragsverarbeitungsvertrag nach DSGVO/GDPR. Es beschreibt, welche Punkte Harpocrypt fuer NGO-/B2B-Piloten beantworten koennen sollte.

Rollenmodell

Regelfall fuer Organisationskunden:

- Kunde/Organisation: Controller/Verantwortlicher fuer Nutzer, Zweck der Kommunikation, Einladungen und interne Berechtigungen.
- Harpocrypt-Betreiber: Processor/Auftragsverarbeiter fuer Betrieb der Kommunikationsplattform.
- Subprozessoren: Hosting, Push, Mail, Monitoring, Storage, sofern genutzt.

Abweichungen muessen projektspezifisch dokumentiert werden, z.B. wenn Harpocrypt eigene Zwecke verfolgt oder Supportdaten eigenstaendig auswertet.

Gegenstand der Verarbeitung

Bereitstellung eines einladungsbasierten Organisationschats mit Ende-zu-Ende-Verschluesselung, Policies, Push-Benachrichtigung, Device-Verwaltung, Recall, Remote-Wipe-Unterstuetzung und AdminWeb.

Art und Zweck

- Nutzer- und Device-Verwaltung.
- Zustellung verschluesselter Nachrichten und Metadaten.
- Verwaltung von Policies, Einladungen, Org-Status und Demo-/Pilotprozess.
- Sicherheits- und Betriebslogging.
- Support und Incident Response.
- Abrechnung und Vertragsverwaltung, falls spaeter aktiviert.

Kategorien personenbezogener Daten

- Organisationsdaten: Name, OrgId, Domain, Status, Pilotzeitraum.
- Nutzerdaten: Displayname, E-Mail, Rolle, UserId, Aktivstatus.
- Device-Daten: DeviceId, Plattform, Public Keys, Attestation, Revoke-Status.
- Kommunikationsmetadaten: ThreadId, MessageId, Sender, Empfaenger, Zeitstempel, PolicyId, Read-State.
- Pushdaten: Push Token, Plattform, Tokenstatus.
- Betriebsdaten: IP/Request-Metadaten, Health-/Error-Logs, Audit Events.
- Demo-/Salesdaten: Firmenname, OrgAdmin-Mail, Ansprechpartner, Branche, User-Anzahl, Use Case.

Chat-Inhalte, Attachments und Voice-Daten sollen serverseitig nur verschluesselt vorliegen.

Kategorien betroffener Personen

- Nutzer der Kundenorganisation.
- OrgAdmins und PlatformAdmins.
- Ansprechpartner in Demo-/Pilotprozessen.
- Support- und Betriebskontakte.

Weisungen

Harpocrypt verarbeitet personenbezogene Daten nur nach dokumentierter Weisung des Kunden, soweit keine gesetzliche Pflicht entgegensteht. Weisungen koennen sich aus Vertrag, AdminWeb-Aktionen, Supporttickets und dokumentierten Incident-Freigaben ergeben.

TOM-Verweis

Die technischen und organisatorischen Massnahmen sind in docs/technical-organisational-measures.md beschrieben. Aenderungen muessen den Schutz nicht wesentlich verschlechtern.

Subprozessoren

Subprozessoren sind in docs/subprocessors.md aufgefuehrt. Neue Subprozessoren sollten vor Einsatz mit angemessener Frist angekuendigt werden, damit Kunden widersprechen koennen.

Loeschung und Rueckgabe

Nach Vertragsende wird nach Wahl des Kunden:

- ein technischer Export der verfuegbaren Metadaten bereitgestellt, soweit Produkt und Vertrag dies vorsehen, oder
- personenbezogene Daten werden nach dem Loeschkonzept geloescht.

Backups werden gemaess Retention-Zeitplan ueberschrieben. Sofortige selektive Loeschung aus bestehenden Backups ist nicht als Standard zugesagt und muss im Vertrag konkret geregelt werden.

Unterstuetzung des Controllers

Harpocrypt unterstuetzt angemessen bei:

- Betroffenenrechten, soweit technisch moeglich.
- Security Incidents und Datenschutzverletzungen.
- DPIA/DSFA-Zuarbeit fuer sensible Piloten.
- Nachweisen zu TOMs, Subprozessoren, Retention und Betriebsregion.

Audit und Nachweise

Fuer Piloten koennen folgende Nachweise bereitgestellt werden:

- Security/Privacy Whitepaper.
- TOMs.
- Subprozessorenliste.

- Backup/Restore- und Incident-Runbooks.
- Pilot-Readiness-Checkliste.
- Externer Security-/Crypto-Review, sobald durchgefuehrt.

Offene Punkte vor Vertragseinsatz

- Juristische Finalisierung nach Land, Vertragsmodell und Rolle.
- Datenloesch-/Exportumfang produktiv technisch finalisieren.
- Subprozessoren final mit Regionen und Transfergrundlagen befuellen.
- AuditService-Produktionsbetrieb entscheiden.
- Support-SLA und Incident-Kommunikationsfristen festlegen.

Quellen

- European Commission: Data controller or data processor

https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_en

- European Data Protection Board: Data controller or data processor

https://www.edpb.europa.eu/sme-data-protection-guide/data-controller-data-processor_en

- GDPR Article 28 via EUR-Lex

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679