# Incident Response Runbook

Stand: 2026-06-15

Dieses Runbook deckt die wichtigsten Pilotfaelle ab. Es ist kein Ersatz fuer ein vollstaendiges ISMS, aber ausreichend fuer kontrollierte NGO-/B2B-Piloten.

## Rollen

- Incident Lead: entscheidet Prioritaet, Kommunikation und Abschluss.
- Technical Lead: prueft Logs, Healthchecks, Datenbank und Servicezustand.
- Customer Contact: informiert OrgAdmin oder Pilotansprechpartner.
- Security Reviewer: prueft nachgelagert, ob Security-/Compliance-Massnahmen noetig sind.

## Severity

| Severity | Beispiel | Zielreaktion |
|---|---|---|
| SEV1 | Datenverlust, breite Nichtverfuegbarkeit, vermuteter Schluessel-/Token-Leak | sofort |
| SEV2 | einzelne Org blockiert, Push/Sendefehler breit, Migration offen | unter 1 Stunde |
| SEV3 | einzelner User ohne Device, fehlerhafte Einladung, einzelne Demo-Anfrage | naechster Werktag |

## Device verloren

- Org im AdminWeb oeffnen.
- Betroffenen User oder Device identifizieren.
- Device widerrufen.
- Remote Wipe ausloesen, falls verfuegbar und sinnvoll.
- Wenn kein aktives Device mehr vorhanden ist: neue Einladung erstellen.
- Testen: neue Gruppennachrichten duerfen nicht an das widerrufene Device gehen.
- Incident dokumentieren.

## Mitarbeiter ausgeschieden

- Alle Devices des Users widerrufen.
- Remote Wipe fuer betroffene Devices anfordern.
- User offboarden oder deaktivieren, falls im AdminWeb verfuegbar.
- Gruppenzustellung testen.
- Falls OrgAdmin betroffen ist: neuen OrgAdmin einladen und MFA einrichten.
- Rollen, Policies und offene Invites pruefen.

# Organisation sperren

- AdminWeb Organisationen oeffnen.
- Org auf Gesperrt setzen.
- Erwartung testen: Mobile bekommt keine neuen Tokens, Registrierung und OrgAdmin-Login werden blockiert.
- Keine automatische Datenloeschung erwarten.
- Bei Vertragsende separat Loesch-/Exportprozess starten.
- Bei Reaktivierung Org auf Active setzen oder Pilot verlaengern.

# Migration offen

- Deployment stoppen.
- Betroffenen Service und Datenbank identifizieren.
- Backup-Zeitpunkt pruefen.
- Migration anwenden oder Service auf kompatible Version zurueckrollen.
- /health/ready pruefen.
- Smoke-Test ausfuehren.

Preflight vor erneuter Freigabe:

```
.\scripts\ops\harpocrypt-backup-preflight.ps1 -ConfigPath .\scripts\ops\backup-preflight.local.json
-OutputPath .\ops-reports\incident-backup-preflight-$(Get-Date -Format yyyyMMdd-HHmmss).md
```

# Sendefehler oder Key-Lookup fehlgeschlagen

- Logs auf messaging event=send.failed und directory event=key_lookup.failed filtern.
- Empfaenger pruefen: aktiver User, aktives Device, Public Keys vorhanden.
- Gruppenmitgliedschaft pruefen.
- Bei fehlendem Device User neu einladen oder aus Gruppe entfernen.
- Testnachricht senden.

# Verdacht auf Datenschutzverletzung oder Security Breach

Dieser Abschnitt ist ein operativer Pruefpfad und keine Rechtsberatung. Sobald personenbezogene Daten betroffen sein koennten, muessen Datenschutzverantwortliche, Legal/DPO oder externe Beratung einbezogen werden.

- Incident Lead und Technical Lead benennen.
- Betroffene Systeme, Organisationen, Nutzergruppen und Zeitraum eingrenzen.
- Pruefen, ob Chat-Klartexte betroffen sein koennen oder nur Metadaten/Betriebsdaten.
- Audit Events, App Service Logs, Datenbankzugriffe und Deployment-/Config-Aenderungen sichern.
- Potenziell betroffene Secrets, Tokens oder Credentials sofort rotieren oder sperren.
- Risiko fuer Rechte und Freiheiten betroffener Personen einschaetzen.
- Kunden/Controller informieren, wenn Harpocrypt als Processor/Auftragsverarbeiter handelt.
- Mit Controller/Legal/DPO pruefen, ob eine Meldung an Aufsichtsbehoerde oder Betroffene erforderlich ist.
- Kommunikationsentwurf vorbereiten: Fakten, Zeitraum, betroffene Datenarten, Massnahmen, Restrisiko.

- Post-Incident Review mit Root Cause, Fixes, Preventive Actions und Dokumentation abschliessen.

Hinweis: Die EDPB Guidelines 9/2022 behandeln Personal-Data-Breach-Notifications unter GDPR. Fuer konkrete Fristen und Pflichten ist die Rolle im jeweiligen Kundenverhaeltnis massgeblich.

# Abschluss

Jeder Incident wird mit diesen Feldern dokumentiert:

- Datum und Zeitraum.
- Betroffene Org/User/Services.
- Ursache oder wahrscheinlichste Ursache.
- Massnahmen.
- Kundenauswirkung.
- Follow-up-Aufgaben.