Data Breach Response Plan

Data Breach Response Plan

> **Organization:** Bilko — Balkan Accounting SaaS **Document Number:** IRP-BILKO-001 **Version:** 1.0 **Date:** 2026-02-23 **Author:** Compliance Architect **Status:** Draft **Reviewers:** DPO, Legal Counsel, Engineering Lead, CEO **Next Review:** 2026-08-23 **Classification:** Confidential — Restricted Distribution

Document History

Version	Date	Author	Changes
0.1	2026-02-23	Compliance Architect	Initial draft — three-jurisdiction notification requirements RS/BA/HR

IMPORTANT — Keep This Document Accessible

> This plan must be accessible even when systems are down. Maintain offline copies and ensure key contacts are saved in personal phones. Key offline contacts: compliance@bilko.io | security@bilko.io | dpo@bilko.io

---

1. Incident Classification

Severity	Definition	Response Team	Max Time to Classify

P1 — Critical	Confirmed breach of Restricted/Confidential data (tax IDs, IBAN, financial records) affecting any number of data subjects; OR active system compromise	Full IRT + Management + Legal	1 hour
P2 — High	Suspected breach with evidence; or confirmed breach of Internal data; or targeted attack detected	Core IRT + Security Lead	2 hours
P3 — Medium	Security event with potential for breach; precautionary action required	Security team	8 hours
P4 — Low	Security anomaly, no confirmed breach	Security team	Next business day

72-hour notification trigger: P1 and P2 MUST be assessed for regulatory notification obligation across all active jurisdictions (HR: AZOP; RS: Poverenik; BA: AZLP).

Financial data sensitivity note: Bilko handles invoices with national tax IDs (PIB/JMBG/OIB/JIB) and IBAN numbers. Any breach exposing these fields is automatically P1 — tax identity theft has severe consequences for data subjects.

---

2. Detection Mechanisms

Detection Method	Tool	Responsible	Alert Channel
Error rate spike	Sentry	Platform team	Slack #alerts
Railway API/CPU anomalies	Railway metrics	Platform team	Slack #alerts
Failed authentication spike (>10 in 1h)	Auth service logs	Platform team	Slack #alerts
Cloudflare WAF block spike	Cloudflare dashboard	Platform team	Email
Audit log anomalies (unusual DELETE patterns)	LoggedAction monitoring	Security team	Slack #alerts
Third-party notification	Vendor contacts us	Security email	security@bilko.io
User-reported	Support ticket	Support team	Escalate to security
Penetration test finding	External pen tester	Security team	Direct report

24/7 security contact: security@bilko.io | compliance@bilko.io

---

3. Response Team Roles & Contacts

Role	Primary	Backup	Email
Incident Commander	CEO (Alem)	Engineering Lead	alem@alai.no
Security Lead	Compliance Architect	Engineering Lead	security@bilko.io
Engineering Lead	Lead Developer	—	engineering@bilko.io
DPO (GDPR/ZZPL/ZZLP)	TBD	Compliance Architect	dpo@bilko.io
Legal Counsel	External (TBD)	—	legal@bilko.io
Communications	CEO	—	alem@alai.no

External regulatory contacts (72-hour notification recipients):

Jurisdiction	Authority	Contact	When
Croatia (HR)	AZOP — Agencija za zaštitu osobnih podataka	azop@azop.hr / https://azop.hr/prijavapovrede	P1/P2 within 72h (GDPR Art. 33)
Serbia (RS)	Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti	office@poverenik.rs / https://www.poverenik.rs	P1/P2 within 72h (ZZPL Art. 56)
Bosnia & Herzegovina (BA)	AZLP — Agencija za zaštitu ličnih podataka BiH	info@azlp.ba / https://www.azlp.ba	P1/P2 within 72h (best practice)

Notify ALL jurisdictions where affected data subjects reside. If a breach affects data from multiple countries, notify all relevant authorities simultaneously.

---

4. Response Procedures by Phase

Phase 1: Detection & Identification (0–1 hour)

Goal: Confirm whether a breach occurred and scope it.

```
Step 1.1 — ALERT RECEIVED
  □ Log initial alert time: _________________
  □ Create incident channel: #incident-{DATE}-{N}
  □ Assign to security lead
  □ Start incident log (chronological — everything goes in the log)
```

```
Step 1.2 — INITIAL ASSESSMENT (within 30 minutes)
  □ What triggered the alert?
  □ Is this a false positive? (if YES → close P4, document)
  □ What systems are affected? (api.bilko.io, Railway DB, Cloudflare R2, SEF/HR-FISK
connections)
  □ Is the attack/leak ongoing?
  □ What data categories potentially affected? (tax IDs, IBAN, invoice data, user credentials)
  □ Which jurisdictions are affected? (RS, BA, HR, or multiple)

Step 1.3 — CLASSIFY INCIDENT
  □ Assign severity: P1 / P2 / P3 / P4
  □ Notify Incident Commander (CEO)
  □ If P1/P2: Activate full IRT immediately
  □ If P3/P4: Notify Security Lead

Step 1.4 — EVIDENCE PRESERVATION (CRITICAL — before containment if safe)
  □ Export Railway logs (30-day window around incident)
  □ Export Cloudflare logs
  □ Export Sentry error timeline
  □ Query LoggedAction: SELECT * FROM logged_actions WHERE action_timestamp > [incident_start]
  □ Screenshot anomalous metrics
  □ DO NOT wipe or restart affected systems until forensics complete
```

Exit criteria: Incident classified, IRT assembled, evidence preserved, 72h clock started if P1/P2.

Phase 2: Containment (1–4 hours)

Goal: Stop the breach. Prevent further data exposure.

```
Step 2.1 — IMMEDIATE CONTAINMENT
  □ Revoke all JWT refresh tokens (DELETE FROM refresh_tokens — forces re-login for all users)
  □ Block malicious IP at Cloudflare WAF
  □ Disable compromised API endpoint if applicable
  □ Rotate JWT_SECRET and JWT_REFRESH_SECRET (all active sessions invalidated)
  □ Rotate FIELD_ENCRYPTION_KEY if database field encryption compromised
  □ Isolate affected Railway services if active exfiltration

Step 2.2 — SCOPE ASSESSMENT
  □ Which data was accessed/exfiltrated? (query LoggedAction + Railway logs)
```

```
  □ Which data subjects affected? (query: SELECT COUNT(*) and list affected organizationIds)
  □ What jurisdictions affected? (RS data subjects? BA? HR?)
  □ What time period? (from: ___ to: ___)
  □ Were tax IDs (PIB/JMBG/OIB/JIB) or IBAN exposed?
  □ Were authentication credentials (password hashes) exposed?
  □ Draft scope statement for DPO and legal review

Step 2.3 — ASSESS CONTAINMENT IMPACT
  □ What services are disrupted by containment actions?
  □ Inform support team of expected user disruption
  □ Prepare user communication if service unavailability expected
```

Exit criteria: Active threat contained, no ongoing exfiltration, scope defined, 72h countdown tracked.

Phase 3: Eradication (4–24 hours)

Goal: Remove root cause. Ensure attacker completely out.

```
Step 3.1 — ROOT CAUSE ANALYSIS
  □ How did the attacker gain access? (SQL injection? JWT bypass? Compromised credentials?
Cloudflare misconfiguration?)
  □ Was there a vulnerability in Prisma query construction?
  □ Was org-scoping WHERE clause bypassed?
  □ How long was access maintained?
  □ Were other organizations' data accessible?

Step 3.2 — REMEDIATE ROOT CAUSE
  □ Apply security patch
  □ Fix vulnerability (e.g., missing org-scope, Zod bypass, rate limit bypass)
  □ Remove any unauthorized database entries or backdoors
  □ Rotate all secrets and API keys

Step 3.3 — VERIFICATION
  □ Run Playwright security test suite
  □ Verify org-scoping isolation tests pass
  □ Verify RBAC tests pass
  □ Confirm no persistence mechanisms
```

Phase 4: Recovery (24–72 hours)

Goal: Restore systems safely.

```
Step 4.1 — SAFE RESTORATION
  □ Deploy patched version
  □ Rotate ALL credentials on affected systems
  □ Enable enhanced monitoring for 30 days post-recovery
  □ Verify data integrity (compare LoggedAction against expected state)
  □ Re-enable services in stages

Step 4.2 — STAKEHOLDER UPDATES
  □ Update incident channel with progress
  □ Brief CEO
  □ Prepare regulatory notifications (see §5)
  □ Prepare customer communication if applicable
```

Phase 5: Post-Incident (72 hours – ongoing)

```
Step 5.1 — POST-MORTEM (within 5 business days)
  □ Blameless post-mortem meeting
  □ Complete timeline of events
  □ Root cause analysis (5 Whys)
  □ What went well / what failed
  □ Action items with owners and deadlines

Step 5.2 — REGULATORY COMPLIANCE
  □ All regulatory notifications filed (see §5)
  □ Data subject notifications sent if required
  □ DPA customer notifications
  □ Insurance claim filed

Step 5.3 — REMEDIATION TRACKING
  □ All action items in issue tracker
  □ Weekly review for 4 weeks
  □ Update DPIA with lessons learned
  □ Update this response plan
```

---

5. Notification Requirements

5.1 Croatia — AZOP (GDPR Art. 33 — 72 hours)

Legal basis: GDPR Regulation (EU) 2016/679, Article 33 **Required if:** Breach likely to result in a risk to rights and freedoms of natural persons **Deadline:** Within **72 hours** of becoming aware (not confirmed — aware) **Partial notification allowed:** Submit what's known within 72h, supplement later

Authority: AZOP — Agencija za zaštitu osobnih podataka **Portal:** https://azop.hr/prijavapovrede **Email:** azop@azop.hr **DPO submits:** dpo@bilko.io

Required information:

- Nature of breach (categories, number of data subjects, number of records)
- DPO contact details
- Likely consequences
- Measures taken or proposed

5.2 Serbia — Poverenik (ZZPL Art. 56 — 72 hours)

Legal basis: Zakon o zaštiti podataka o ličnosti, Article 56 **Required if:** Breach likely to result in risk to rights and freedoms of individuals **Deadline:** Within **72 hours** of becoming aware

Authority: Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti **Portal:** https://www.poverenik.rs **Email:** office@poverenik.rs **Address:** Bulevar kralja Aleksandra 15, 11000 Belgrade, Serbia

5.3 Bosnia & Herzegovina — AZLP (72 hours — best practice)

Legal basis: Zakon o zaštiti ličnih podataka BiH — breach notification not explicitly mandated in same detail as GDPR, but best practice is 72-hour notification following GDPR standard. **Deadline:** 72 hours (voluntary/best practice)

Authority: AZLP — Agencija za zaštitu ličnih podataka Bosne i Hercegovine **Email:** info@azlp.ba **Address:** Hamdije Čemerlića 2/VI, 71000 Sarajevo, Bosnia & Herzegovina

5.4 Data Subject Notification (GDPR Art. 34 / ZZPL Art. 57)

Required if: Breach likely to result in HIGH risk to data subjects **Timeline:** Without undue delay
Method: Direct email to affected users — individual, not public announcement

Financial data breach — assess HIGH risk if:

- Tax IDs (PIB/JMBG/OIB/JIB) exposed — identity theft risk
- IBAN exposed — financial fraud risk
- Password hashes exposed (weak hashing) — credential stuffing risk
- Note: bcrypt-hashed passwords with cost=12 are computationally infeasible to crack — assess as LOW risk even if hashes exposed

5.5 Multi-Jurisdiction Notification Checklist

```
□ Identify all affected data subjects by country
□ If Croatian users affected → notify AZOP within 72h
□ If Serbian users affected → notify Poverenik within 72h
□ If BiH users affected → notify AZLP within 72h (best practice)
□ If HIGH risk to any users → notify affected users directly (no undue delay)
□ If DPA customers affected → notify per DPA contract terms
□ Document all notifications with timestamp and reference number
```

---

6. Communication Templates

6.1 Internal Incident Alert

```
Subject: [INCIDENT P{SEVERITY}] Security Incident — Bilko — {DATE} {TIME}

Team,

Security incident detected. Details:

Incident ID: INC-BILKO-{DATE}-{N}
Severity: P{SEVERITY}
Detected: {DATE} {TIME} UTC
```

```
Jurisdictions potentially affected: {RS / BA / HR}
Data potentially affected: {tax IDs / IBAN / credentials / invoice data}
Status: ACTIVE — Containment in progress

Incident Commander: Alem (CEO)
Incident channel: #incident-{DATE}-{N}

72h regulatory notification clock started: {DATE} {TIME} UTC
Notification deadlines:
  - AZOP (HR): {DATE+72h}
  - Poverenik (RS): {DATE+72h}
  - AZLP (BA): {DATE+72h}

Do NOT discuss on public channels, with customers, or social media.
All communications through Alem.

Next update: {TIME} UTC
```

6.2 Data Subject Notification (Croatian / English)

```
Subject: Važna sigurnosna obavijest o vašem računu / Important security notice

Poštovani {IME} / Dear {FIRST_NAME},

Bilko (bilko.io) vas obavještava o sigurnosnom incidentu koji je mogao utjecati
na vaš račun.

Što se dogodilo / What happened:
Dana {DATUM}, saznali smo za neovlašteni pristup našim sustavima koji je mogao
izložiti vaše osobne podatke.

Koji podaci su zahvaćeni / Data potentially affected:
{KATEGORIJE_PODATAKA}

Što smo poduzeli / What we did:
- {MJERA_1}
- {MJERA_2}

Što trebate učiniti / What you should do:
```

```
- Promijenite lozinku na bilko.io / Change your password at bilko.io
- Omogućite dvofaktorsku autentikaciju / Enable two-factor authentication
- Pratite sumnjive aktivnosti / Monitor for suspicious activity

Za više informacija / For more information:
DPO: dpo@bilko.io
Privacy: bilko.io/privacy

Ispričavamo se za uzrokovanu neugodnost.
We sincerely apologize for any concern this may cause.

Bilko tim / Bilko Team
DPO: dpo@bilko.io
```

6.3 Regulatory Notification Draft (GDPR Art. 33 — for AZOP, Poverenik, AZLP)

```
To: {AUTHORITY_NAME} — {AUTHORITY_EMAIL}
From: {DPO_NAME}, DPO — Bilko (bilko.io)
Date: {DATE} {TIME} UTC

NOTIFICATION OF PERSONAL DATA BREACH

1. Nature of the breach:
   On {DATE}, we became aware of {unauthorized access to / accidental disclosure of}
   personal data processed by Bilko. The breach {is/was} {ONGOING/CONTAINED}.

2. Categories of data subjects and approximate numbers:
   - Data subjects: {NUMBER} (estimated)
   - Categories: {user account data / tax IDs (PIB/JMBG/OIB/JIB) / IBAN / invoice data}
   - Records: {NUMBER} (estimated)
   - Countries of affected data subjects: {RS / BA / HR}

3. Contact details of DPO:
   Name: {DPO_NAME}
   Email: dpo@bilko.io
   Organization: Bilko (bilko.io)

4. Likely consequences:
```

```
   {ASSESSMENT — e.g., "Tax ID exposure creates risk of identity theft; IBAN exposure creates risk of financial fraud"}

5. Measures taken or proposed:
   Immediate: {CONTAINMENT_MEASURES}
   Ongoing: {ONGOING_MEASURES}
   Planned: {REMEDIATION_MEASURES}

6. Note: This is a {complete / preliminary — supplementary notification to follow} report.

[DPO Signature]
{DPO_NAME}
dpo@bilko.io
```

---

7. Evidence Preservation

```
Evidence checklist:
□ Railway log export: all services, 30-day window around incident
□ Cloudflare log export: WAF events, access logs
□ Sentry: error events export
□ LoggedAction query: all mutations during incident window
  SELECT * FROM logged_actions WHERE action_timestamp BETWEEN '{start}' AND '{end}'
□ PostgreSQL: pg_stat_activity snapshot, connection history
□ Authentication logs: failed login attempts, token usage

Chain of custody:
- SHA-256 hash all exported files immediately after collection
- Record: filename, hash, collector, timestamp
- Storage: encrypted archive, access restricted to IRT
```

---

8. Drill Schedule

Drill Type	Frequency	Participants	Scenario
Tabletop exercise	Quarterly	Full IRT + CEO	Tax ID breach / IBAN exposure / credential stuffing

Drill Type	Frequency	Participants	Scenario
Notification drill	Semi-annual	DPO + Legal	72-hour multi-jurisdiction notification dry run
Technical response	Annual	Engineering + Security	Simulated org-scope bypass in staging

Last drill: Not yet conducted — schedule within 30 days of product launch **Drill coordinator:** Compliance Architect (security@bilko.io)

Approval

Role	Name	Date	Signature
Author	Compliance Architect	2026-02-23	
DPO			
Legal Counsel			
CEO			

Revision #9
Created 2026-02-23 12:03:01 UTC by John
Updated 2026-05-25 07:32:32 UTC by John