Breach Response Plan

Data Breach Response Plan

> **Organization:** Bilko — Balkan Accounting SaaS **Document Number:** IRP-SEC-001 **Version:** 1.0 **Date:** 2026-02-23 **Author:** DPO / CTO **Status:** Draft — requires DPO approval before launch **Reviewers:** CTO, DPO, CEO **Classification:** Confidential

Document History

Version	Date	Author	Changes
0.1	2026-02-23	DPO	Initial breach response plan — three-jurisdiction (RS, BA, HR)

---

1. Incident Response Team

Role	Person	Contact	Responsibility
Incident Commander	CTO	cto@bilko.io	Technical response, containment, investigation
DPO	DPO	dpo@bilko.io	Regulatory notification, data subject communication
CEO	CEO	ceo@bilko.io	Stakeholder comms, business decisions, media
Legal Counsel	External	legal@bilko.io	Regulatory advice, notification drafting
On-call Engineer	Rotates	Slack: #bilko-incidents	First responder — detection, initial containment

Escalation order: On-call → CTO → DPO → CEO

2. What Constitutes a Breach

A personal data breach is any security incident leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Examples

Incident	Breach?	Severity
Unauthorized access to a customer's invoice data	YES	HIGH
Exposure of PIB/JMBG/OIB/JIB tax IDs	YES	CRITICAL
IBAN numbers exposed	YES	CRITICAL
Railway DB credentials exposed	YES — potential breach	CRITICAL
Server error logs contain email addresses	YES (minor)	LOW
Employee accidentally emails invoice to wrong address	YES	MEDIUM
Unsuccessful SQL injection attempt (no data accessed)	NO — log and monitor	LOW
DDoS attack — service unavailable, no data accessed	NO	N/A

3. Response Timeline

```
timeline
    title Breach Response Timeline (72 hours)
    section Hour 0
        Detection : Alert fires (monitoring, customer report, employee discovery)
        Verification : Is this a real breach? Contain false positives.
    section Hour 1-4
        Containment : Block attacker, revoke credentials, isolate affected systems
        Assessment : What data was accessed? How many records? Which jurisdictions?
    section Hour 4-24
        Investigation : Root cause analysis. Audit logs (LoggedAction table).
        Internal notification : CTO, DPO, CEO briefed.
```

```
    section Hour 24-48
        Regulatory notification : Poverenik (RS), AZLP (BA), AZOP (HR) if required
        Evidence preservation : Immutable audit trail extracted. Logs archived.
    section Hour 48-72
        Data subject notification : If high risk to individuals
        Remediation : Patch deployed. Controls improved.
    section After 72h
        Post-mortem : Root cause documented. Prevention measures implemented.
        Follow-up reporting : Supervisory authorities updated if required.
```

---

4. Regulatory Notification Requirements

4.1 Notification Thresholds

Jurisdiction	Law	Notify Authority	Deadline	Condition
Croatia	GDPR Art. 33	AZOP (azop.hr)	**72 hours**	Unless breach is unlikely to result in risk to rights/freedoms
Serbia	ZZPL Art. 56	Poverenik (poverenik.rs)	**72 hours**	Applies analogously (GDPR-aligned law)
Bosnia & Herzegovina	ZZLP BiH Art. 20	AZLP (azlp.gov.ba)	**Best practice 72 hours** (law less specific)	Recommended to align with GDPR practice

Default: Notify all three authorities unless legal counsel advises otherwise.

4.2 Authority Contact Details

Authority	Jurisdiction	Website	Notification Method
Agencija za zaštitu osobnih podataka (AZOP)	Croatia	azop.hr	Online form + email: azop@azop.hr
Poverenik za informacije od javnog značaja	Serbia	poverenik.rs	Online form at poverenik.rs/zastitapodataka
Agencija za zaštitu ličnih podataka (AZLP)	Bosnia & Herzegovina	azlp.gov.ba	Email: azlp@azlp.gov.ba

4.3 Notification Content (per GDPR Art. 33 / ZZPL Art. 56)

Required information for supervisory authority notification:

```
1. Nature of the breach (what happened, how discovered)
2. Categories and approximate number of data subjects affected
3. Categories and approximate number of records affected
4. Contact details of DPO: dpo@bilko.io
5. Likely consequences of the breach
6. Measures taken or proposed to address the breach
```

Template: See Section 7.1

4.4 Data Subject Notification (GDPR Art. 34)

Notify affected individuals "without undue delay" if breach is **likely to result in high risk** to their rights and freedoms.

High risk triggers for Bilko data:

- Tax ID (PIB/JMBG/OIB/JIB) exposure — identity theft risk
- IBAN exposure — financial fraud risk
- Full invoice data exposure — business espionage risk

---

5. Response Procedures

5.1 Detection & Verification (0–1 hour)

Detection sources:

- Sentry error tracking — unusual error patterns
- Railway logs — unexpected query volumes or failed auth attempts
- Cloudflare WAF alerts — unusual traffic patterns
- Customer complaint — "I can see another company's data"
- Employee discovery

Verification steps:

1. Access Railway logs and Cloudflare analytics

2. Query LoggedAction table for anomalous access patterns:

```
SELECT userId, orgId, action, tableName, ipAddress, COUNT(*)
FROM "LoggedAction"
WHERE timestamp > NOW() - INTERVAL '1 hour'
GROUP BY userId, orgId, action, tableName, ipAddress
ORDER BY COUNT(*) DESC;
```

3. Confirm whether actual personal data was accessed (not just attempted)
4. Declare incident: `#bilko-incidents` Slack channel + page Incident Commander

5.2 Containment (1–4 hours)

Immediate actions (within 30 minutes of confirmation):

- ☐ Revoke affected user sessions (invalidate JWT refresh tokens in DB)
- ☐ If credentials compromised: rotate all Railway environment secrets
- ☐ If SQL injection: enable Railway maintenance mode temporarily
- ☐ If insider threat: suspend user account, preserve audit logs
- ☐ If third-party compromise: revoke API keys to SEF/FINA/Sentry

Preserve evidence:

- Extract relevant LoggedAction rows to immutable storage (S3 / local encrypted archive) before any system changes
- Do not delete logs, rotate secrets in place (old secret documented in Vaultwarden with timestamp)

5.3 Assessment (4–24 hours)

Determine scope:

- Which organizations were affected?
- Which data categories? (check against Data Inventory in DPIA)
- Approximate number of data subjects?
- Which jurisdictions? (RS, BA, HR, or all?)
- Was data exfiltrated, or only accessed?
- What is the risk to data subjects?

Severity classification:

Severity	Criteria	Response

CRITICAL	Tax IDs, IBAN, financial amounts exfiltrated	Notify all authorities within 24h; notify all affected data subjects
HIGH	Invoice metadata accessed across tenant boundary	Notify authorities within 72h; assess individual notification
MEDIUM	Email/name exposure, no financial data	Notify authorities if >250 records; assess individual notification
LOW	Single record, no sensitive data, no exfiltration	Document internally; no mandatory notification

5.4 Regulatory Notification (24–72 hours)

1. DPO drafts notification using template in Section 7.1
2. Legal counsel reviews
3. CEO approves
4. DPO submits to AZOP (HR), Poverenik (RS), AZLP (BA) simultaneously
5. Log submission timestamp and reference numbers received

If full details not available within 72 hours: Submit initial notification with known information and state investigation is ongoing. Supplement with additional notifications as information becomes available (GDPR Art. 33(4) allows phased notification).

5.5 Data Subject Notification

If high risk determined (Section 4.4):

1. Identify email addresses of all affected data subjects
2. DPO drafts data subject notification (see Section 7.2)
3. Send via Bilko email account — do not use marketing email tools
4. Provide clear guidance on what to do (change password, monitor bank statements)

---

6. Post-Incident

6.1 Post-Mortem

Complete within 2 weeks of incident resolution. Template: `OPERATIONS/post-mortem.md`

- Root cause (5 Whys)
- Timeline reconstruction from LoggedAction + logs
- What controls failed?
- What controls worked?

- Action items with owners and deadlines

6.2 Regulatory Follow-Up

- AZOP, Poverenik, AZLP may request follow-up information within 3 months
- Maintain incident dossier for minimum 3 years (GDPR Art. 33(5))
- Document: what happened, who was notified, when, remediation taken

6.3 Insurance

- Notify cyber insurance provider if breach exceeds threshold (per policy)
- Preserve evidence for potential claims

---

7. Notification Templates

7.1 Supervisory Authority Notification (English — adapt per jurisdiction)

```
Subject: Personal Data Breach Notification — Bilko Cloud Accounting — [DATE]

To: [AZOP / Poverenik / AZLP]

We are reporting a personal data breach pursuant to [GDPR Art. 33 / ZZPL Art. 56 / ZZLP BiH Art. 20].

Controller: Bilko d.o.o. | dpo@bilko.io | +[phone]
DPO Contact: dpo@bilko.io

1. NATURE OF BREACH
[Description: what happened, when discovered, how]

2. DATA SUBJECTS AFFECTED
Approximate number: [NUMBER]
Categories: [accountants / business owners / invoice recipients]

3. RECORDS AFFECTED
Categories: [tax IDs / IBAN / invoice amounts / email addresses]
```

```
Approximate number: [NUMBER]

4. LIKELY CONSEQUENCES
[Identity theft risk / financial fraud risk / business espionage risk]

5. MEASURES TAKEN
[Containment steps, credential rotation, patch deployed]
[Ongoing investigation]

6. FURTHER INFORMATION
This notification is [complete / preliminary – further information to follow].

[DPO Name]
DPO – Bilko
dpo@bilko.io
```

7.2 Data Subject Notification (Croatian — adapt for RS/BA)

```
Predmet: Obavijest o povredi osobnih podataka – Bilko

Poštovani/a,

Obavještavamo Vas da je Bilko bio izložen sigurnosnom incidentu koji je mogao
utjecati na Vaše osobne podatke.

Što se dogodilo:
[Jednostavan opis – kada, što je bilo pristupljeno]

Koji su Vaši podaci bili zahvaćeni:
[Navesti konkretno: PIB, IBAN, iznosi računa – samo što je relevantno]

Što smo poduzeli:
[Koraci: blokiranje pristupa, obavještavanje AZOP-a, poboljšanje sigurnosti]

Što možete učiniti:
- Promijenite lozinku na bilko.io
- Pratite aktivnosti na bankovnim računima
- Kontaktirajte nas na dpo@bilko.io s pitanjima
```

```
Izvinjenje:
Žao nam je što se ovo dogodilo. Zaštita Vaših podataka naša je prioritetna obveza.

S poštovanjem,
Bilko tim
dpo@bilko.io
```

Approval

Role	Name	Signature	Date
Author	DPO / CTO		2026-02-23
Reviewer (CEO)			
DPO Approval			
Legal Counsel Approval			

Revision #3
Created 2026-02-24 22:50:54 UTC by John
Updated 2026-05-31 20:04:00 UTC by John