DPIA — Data Protection Impact Assessment

Data Protection Impact Assessment (DPIA)

> **Project:** Bilko — Balkan Accounting SaaS **Version:** 1.0 **Date:** 2026-02-23 **Author:** DPO **Status:** Draft — requires DPO sign-off before launch **Reviewers:** CTO, Legal Counsel, DPO **Classification:** Confidential

Document History

Version	Date	Author	Changes
0.1	2026-02-23	DPO	Initial DPIA for Bilko accounting SaaS

---

1. DPIA Necessity Assessment

Is this DPIA mandatory? YES.

Bilko meets multiple high-risk criteria under GDPR Article 35 and equivalent provisions in ZZPL (Serbia Art. 54) and ZZLP BiH (Art. 17a):

Criterion	Applies	Reason
Large-scale processing of sensitive data	YES	Tax IDs (PIB, JMBG, OIB, JIB) qualify as identification data processed at scale
Systematic processing of personal data	YES	Core business function — every user's financial data processed continuously

Criterion	Applies	Reason
Processing that determines access to financial services	YES	Accounting data used for tax filings, credit applications, regulatory compliance
Multi-jurisdictional cross-border transfers	YES	RS/BA to EU host (Railway)
Vulnerable data subjects	PARTIAL	Some SMB owners may be natural persons with limited tech literacy

---

2. System Description

System Name: Bilko Cloud Accounting Platform **Controller:** Bilko d.o.o. / Bilko d.o.o. Sarajevo / Bilko d.o.o. Zagreb (per jurisdiction) **Processor(s):** Railway (hosting), Cloudflare (CDN/WAF), Sentry (error tracking) **DPO Contact:** Alem Bašić — alem@alai.no — +47 40 47 42 51

Purpose: Provide cloud-based double-entry accounting, invoicing, expense tracking, VAT reporting, and e-invoicing integration (SEF for RS, HR-FISK for HR) to SMBs in Serbia, Bosnia & Herzegovina, and Croatia.

Lawful basis: Contract performance (Art. 6(1)(b)) for core accounting services; Legal obligation (Art. 6(1)(c)) for tax ID storage and retention periods.

---

3. Data Flows

```
flowchart LR
    subgraph USERS["Data Subjects"]
        OWNER["Business Owner\n(natural person)"]
        CLIENT["Client (Contact)\n(natural person or legal entity)"]
    end

    subgraph BILKO["Bilko Platform"]
        API["Express API\n(Railway EU West)"]
        DB["PostgreSQL\n(Railway EU West)"]
        AUDIT["LoggedAction\nAudit Table"]
    end

    subgraph EXTERNAL["External Integrations"]
```

```
        SEF["SEF Portal\n(Serbia — efaktura.mfin.gov.rs)"]
        HRFISK["HR-FISK\n(Croatia — FINA)"]
        CF["Cloudflare WAF"]
        SENTRY["Sentry\n(Error tracking)"]
    end

    OWNER -->|"Creates account\nEmail, name, OrgPIB"| API
    OWNER -->|"Creates invoice\nBuyer PIB/OIB/JIB/JMBG\nIBAN\nAmounts"| API
    CLIENT -->|"Receives invoice\n(email)"| OWNER
    API --> DB
    API --> AUDIT
    API -->|"e-invoice XML"| SEF
    API -->|"e-invoice XML + FINA cert"| HRFISK
    API -->|"All traffic"| CF
    API -->|"Error traces"| SENTRY
```

Data Inventory

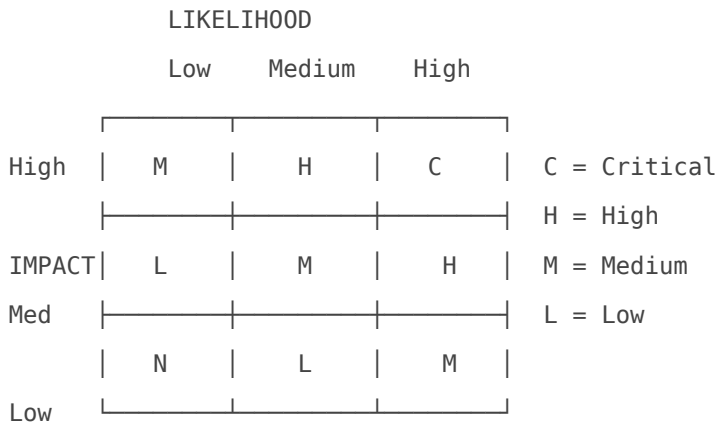
Data Element	Source	Stored	Encrypted	Retention	Jurisdiction
Email address	User registration	YES	No (indexed)	Account lifetime	All
Full name	User registration	YES	No	Account lifetime	All
Organization name	Registration	YES	No	10-11 years	All
PIB (Serbia tax ID)	Invoice creation	YES	**Disk encryption + API controls** (L4-B, See ADR-014)	10 years	RS
JMBG (Serbia personal ID)	Invoice — natural persons	YES	**AES-256-GCM field-level** + HMAC-SHA256 hash (L4-A, See ADR-014)	10 years	RS
OIB (Croatia personal tax ID)	Invoice creation	YES	**AES-256-GCM field-level** + HMAC-SHA256 hash (L4-A, See ADR-014)	11 years	HR
JIB (BiH tax ID)	Invoice creation	YES	**Disk encryption + API controls** (L4-B, See ADR-014)	10-11 years	BA

Data Element	Source	Stored	Encrypted	Retention	Jurisdiction
IBAN	Bank accounts / invoices	YES	**Disk encryption + API masking** (last 4 digits in list views) (L4-B, See ADR-014)	10-11 years	All
Invoice amounts	Invoices	YES	No (NUMERIC 19,4)	10-11 years	All
IP address	Session logs	YES	No	30 days	All
Browser user agent	Session logs	YES	No	30 days	All
Audit trail entries	System	YES	No	10-11 years	All

---

4. Risk Assessment

Risk Matrix



Identified Risks

Risk ID	Risk	Impact	Likelihood	Rating	Mitigation
R-01	Unauthorized access to personal IDs (JMBG/OIB)	High	Medium	**H**	AES-256-GCM field-level encryption (L4-A, ADR-014); RBAC restricts access

Risk ID	Risk	Impact	Likelihood	Rating	Mitigation
R-01b	Unauthorized access to business IDs (PIB/JIB)	Low-Medium	Medium	**M**	Disk encryption + org-scoping + RBAC (L4-B, ADR-014); PIB/JIB are publicly available on gov portals
R-02	Cross-tenant data leak (one org sees another's data)	High	Low	**M**	Prisma org-scoped WHERE on every query; automated test suite
R-03	IBAN exposure enabling financial fraud	Medium	Low	**L**	Disk encryption + API masking (last 4 digits in list views) (L4-B, ADR-014); IBAN is routinely shared for payment
R-04	Breach of invoice data (amounts, buyer/seller details)	High	Low	**M**	TLS 1.3; Railway AES-256 at rest; RBAC
R-05	Railway data center compromise	High	Very Low	**L**	Railway EU West (ISO 27001); DPA signed; encrypted backups
R-06	Insufficient retention — legal/regulatory penalty	High	Medium	**H**	Retention lock prevents deletion; automated alerts before expiry
R-07	Failed SEF/HR-FISK e-invoice — business disruption + fine	High	Medium	**H**	Test environment; idempotent submission; alert on failure
R-08	Employee/insider access to client financial data	Medium	Low	**L**	RBAC; LoggedAction audit trail; background checks for staff
R-09	Account takeover via credential stuffing	High	Medium	**H**	bcrypt 12; rate limiting 5/15min auth; HIBP breach check

Risk ID	Risk	Impact	Likelihood	Rating	Mitigation
R-10	JMBG processed without adequate legal basis	High	Low	**M**	JMBG only accepted when user confirms natural person billing
R-11	Cross-border transfer BA → Railway without adequate mechanism	Medium	Medium	**M**	Standard Contractual Clauses with Railway for BiH users

Residual Risk Assessment

After applying controls in Section 5:

- R-01 (JMBG/OIB): Residual = **Low** (AES-256-GCM field-level encryption + RBAC, ADR-014 Tier 1)
- R-01b (PIB/JIB): Residual = **Low** (disk encryption + org-scoping; data is publicly available on gov registries)
- R-03 (IBAN): Residual = **Low** (disk encryption + API masking; IBAN is routinely shared for payment)
- R-06, R-07, R-09: Residual = **Medium** (operational dependencies remain)
- R-11: Residual = **Low** (SCC in place)

Overall residual risk: MEDIUM — Acceptable with DPO sign-off.

---

5. Mitigation Measures

Control	Addresses	Implementation
AES-256-GCM field-level encryption for JMBG and OIB (L4-A)	R-01, R-10	`prisma-field-encryption` extension — `jmbg` and `oib` fields encrypted before write; `jmbgHash` / `oibHash` HMAC columns for exact-match lookup (See ADR-014)
Disk-level encryption + API controls for PIB, JIB, IBAN (L4-B)	R-01b, R-03	Railway AES-256 disk encryption + org-scoping + RBAC; IBAN masked to last 4 digits in list responses (See ADR-014)
Org-scoped WHERE on all Prisma queries	R-02	Lint rule + automated isolation tests
JWT 15min access + 7day refresh + rotation	R-09	Express auth middleware

Control	Addresses	Implementation
bcrypt cost factor 12	R-09	Password hashing on registration
Rate limiting: 5 auth req / 15min	R-09	`express-rate-limit`
HIBP breach check on registration	R-09	k-anonymity API call
LoggedAction audit trail (append-only)	R-08	Prisma middleware — every write operation
Retention lock (10-11yr minimum)	R-06	`deletedAt` check + age validation before hard delete
DPA with Railway	R-05	Legal — sign before launch
SCCs with Railway (for BiH users)	R-11	Legal — sign before launch
SEF/HR-FISK idempotent submission + retry	R-07	API integration with deduplication key
JMBG consent gate	R-10	UI checkbox: "This invoice is for a natural person"

---

6. Consultation

DPO Consultation

- DPO: Alem Bašić (alem@alai.no, +47 40 47 42 51, ALAI Holding AS org.nr 932 953 736)
- DPIA mandatory per GDPR Art. 35 — DPO must be consulted before processing begins
- DPO appointed: 2026-03-02 (jf. GDPR Art. 37-39 / personopplysningsloven)
- DPO opinion: [PENDING — sign-off required before production launch]

Supervisory Authority Prior Consultation

Prior consultation required if residual risk remains HIGH after all mitigations. Current assessment: MEDIUM — **prior consultation NOT required**, but this must be reasserted when HR-FISK and JMBG features are fully implemented.

Data Subject Consultation

Consideration: SMB owners are sophisticated business users. DPIA does not require data subject consultation for B2B accounting software, but privacy policy must clearly explain tax ID processing.

---

7. Approval & Review

DPO Sign-off Required Before: Any feature that processes PIB, JMBG, OIB, JIB, or IBAN goes to production.

Next DPIA Review: When adding new data categories, new jurisdictions, or new external integrations.

Role	Name	Signature	Date
Author	Alem Bašić		2026-02-23
Reviewer (CTO)			
DPO Approval	Alem Bašić		
CEO Sign-off	Alem Bašić		

Revision #10
Created 2026-02-24 23:50:54 UTC by John
Updated 2026-06-07 19:43:47 UTC by John