Data Protection Impact Assessment (DPIA)

Data Protection Impact Assessment (DPIA)

> **Project:** Bilko — Balkan Accounting SaaS **Processing Activity:** Multi-Tenant Accounting Data Processing (invoices, expenses, VAT, tax filings) **Version:** 1.0 **Date:** 2026-02-23 **Author:** Compliance Architect **DPO:** TBD (dpo@bilko.io) **Status:** Draft **Reviewers:** DPO, Legal Counsel, Engineering Lead **Classification:** Confidential

Document History

Version	Date	Author	Changes
0.1	2026-02-23	Compliance Architect	Initial DPIA — accounting SaaS data processing

---

DPIA Trigger Checklist

#	Trigger	Applies?	Notes
1	Systematic profiling / automated decisions with legal effects	NO	No profiling or automated decisions
2	Large-scale special category data (health, religion, ethnicity)	NO	Financial data is not Art. 9 special category
3	Systematic monitoring of publicly accessible areas	NO	N/A

#	Trigger	Applies?	Notes
4	Biometric or genetic data	NO	N/A
5	Data about vulnerable subjects (children, patients)	PARTIAL	Employees submitting expense claims via employer's Bilko account
6	Innovative technology with unpredictable privacy impact	NO	Standard cloud accounting SaaS
7	Cross-border transfer outside EEA without adequate protection	YES	Serbian (ZZPL) and BiH (ZZLP) data subjects — data processed on EU servers
8	Processing that prevents data subjects from exercising rights	NO	Self-service endpoints provided

DPIA Required: YES **Reason:** Cross-border transfer of RS/BA data subjects to EU-hosted infrastructure; processing of national tax IDs (PIB/JMBG/OIB/JIB) as sensitive identifiers; financial data for thousands of organizations and their counterparties.

---

1. Processing Activity Description

1.1 Activity Overview

Activity Name: Multi-Tenant Accounting Data Processing **System/Product:** Bilko (bilko.io)
Business Unit: Product **Processing Owner:** Engineering Lead (engineering@bilko.io)

Description of Processing: Bilko processes financial and personal data on behalf of business organizations (data controllers) in Serbia, Bosnia & Herzegovina, and Croatia:

1. User account data — email, full name, bcrypt-hashed password, TOTP secret
2. Organization data — legal name, tax ID (PIB/JIB/OIB), address, banking details
3. Contact data — customer/supplier names, tax IDs, email, phone, IBAN
4. Invoice data — invoice numbers, dates, amounts, VAT, payment status
5. Expense data — amounts, categories, descriptions, receipt attachments
6. Transaction data — bank transactions, double-entry debit/credit
7. Audit trail — all mutations logged with user ID, IP, timestamp, old/new values

Business Justification: SMBs in the Balkans lack affordable, compliant cloud accounting software. Processing this data is necessary to deliver the contracted accounting service and meet legal obligations under RS/BA/HR accounting and tax laws.

1.2 Processing Operations

Operation	Data Category	Technology	Location
Collection (registration)	Email, name, password	HTTPS POST, Zod validation	bilko.io — Vercel EU
Collection (invoicing)	Contact data, tax IDs, amounts	HTTPS API	api.bilko.io — Railway EU West
Storage	All categories	PostgreSQL AES-256	Railway EU West (Frankfurt/Paris)
Storage (files)	Receipt PDFs/JPGs	Cloudflare R2 AES-256	Cloudflare EU region
Processing	VAT calculations, reports	Express API, Prisma ORM	Railway EU West
Sharing	Invoice PDFs	SendGrid email	EU region
E-invoice submission	Invoice XML	UBL 2.1 SEF / HR-FISK	Serbia (SEF) / Croatia (FINA)
Deletion / Anonymization	User PII	Soft delete + anonymization	Railway EU West

---

2. Necessity & Proportionality Assessment

2.1 Purposes of Processing

Purpose	Specific Description	Legitimate?
Account authentication	Verify user identity for organization access	YES — contract necessity (Art. 6.1.b)
Invoice generation	Create legally compliant invoices with tax IDs required by law	YES — legal obligation (Art. 6.1.c)
VAT calculation and reporting	Calculate VAT at RS 20% / BA 17% / HR 25%	YES — legal obligation (Art. 6.1.c)
Financial record keeping	Double-entry books required by accounting law	YES — legal obligation (Art. 6.1.c)
Audit trail	Immutable log of financial mutations	YES — legal obligation + legitimate interest (Art. 6.1.c + 6.1.f)
E-invoice submission	Submit to SEF (Serbia) and HR-FISK (Croatia)	YES — legal obligation (Art. 6.1.c)
Invoice email delivery	Deliver invoices to customers	YES — contract necessity (Art. 6.1.b)

2.2 Data Minimization Assessment

Data Element	Collected	Strictly Necessary?	Alternative
`email`	YES	YES — login + invoice delivery	N/A
`fullName`	YES	YES — required on invoices	N/A
`passwordHash`	YES	YES — authentication	N/A (bcrypt hash)
`totpSecret`	YES	YES — 2FA	N/A
`organizationTaxId` (PIB/JIB/OIB)	YES	YES — legally required on invoices	N/A
`organizationIban`	YES	YES — payment reference	N/A
`contactTaxId` (PIB/JMBG/OIB/JIB)	YES	YES — VAT law requires buyer tax ID	N/A
`contactIban`	YES	PARTIAL — needed only for payment features	Collect only when payment active
`clientIp` (audit log)	YES	YES — security, fraud detection	Retain max 30 days for security entries
`userAgent`	NO	NO — not collected	Not collected
`deviceId`	NO	NO — not collected	Not collected

2.3 Lawful Basis

Processing Activity	Lawful Basis	Justification
Account management	Contract — Art. 6.1.b	Necessary to provide the service
Invoice / expense / transaction processing	Legal obligation — Art. 6.1.c	Zakon o PDV + Zakon o računovodstvu
VAT calculation and reporting	Legal obligation — Art. 6.1.c	Mandatory under RS/BA/HR tax laws
Audit trail	Legal obligation + Legitimate interest — Art. 6.1.c + 6.1.f	Accounting law + fraud detection
IP address logging	Legitimate interest — Art. 6.1.f	Security monitoring, 30-day retention
E-invoice submission (SEF/HR-FISK)	Legal obligation — Art. 6.1.c	Mandatory electronic submission
Data retention beyond erasure	Legal obligation — Art. 6.1.c	10-11 year retention per accounting law

---

3. Data Subjects & Categories of Data

3.1 Data Subject Groups

Group	Description	Estimated Volume	Vulnerability
Business owners / admins	SMB owners using Bilko	1-10 per organization	Low
Accountants	Professional accountants on client accounts	1-5 per organization	Low
Employees	Submitting expense claims via employer's account	Variable	Low-Medium
Counterparties	Customers/suppliers appearing on invoices	External to Bilko	Low (financial risk if breached)

3.2 Personal Data Categories

Category	Data Elements	Sensitivity	Classification
Contact	Name, email, phone	Standard	L3 Confidential
Authentication	bcrypt(password), TOTP secret	High	L4 Restricted
Tax identity	PIB, JMBG, OIB, JIB	High	L4 Restricted
Financial	Invoice amounts, IBAN, bank transactions	High	L3 Confidential
Behavioral / Audit	IP address, action timestamps, old/new values	Standard	L2 Internal
Attachments	Receipt PDFs, invoice attachments	Standard-High	L3 Confidential

---

4. Data Processing Purposes & Legal Basis

Processing Purpose	Personal Data Used	Legal Basis	Retention Period
User authentication	email, passwordHash, totpSecret	Contract (Art. 6.1.b)	Until account deletion
Invoice creation and delivery	org name, tax ID, contact name/tax ID/address, amounts	Legal obligation (Art. 6.1.c)	10 years (RS) / 11 years (HR/BA RS entity)
VAT calculation	Invoice amounts, tax rates, tax IDs	Legal obligation (Art. 6.1.c)	10-11 years

Processing Purpose	Personal Data Used	Legal Basis	Retention Period
Expense management	Amounts, descriptions, receipt images	Legal obligation (Art. 6.1.c)	10-11 years
Financial reporting	All financial data	Legal obligation (Art. 6.1.c)	10-11 years
Audit trail	userId, IP, timestamp, changedFields	Legal obligation + Legitimate interest	Financial: 10-11 years; IP/security: 30 days
E-invoice (SEF/HR-FISK)	Invoice XML with buyer/seller data	Legal obligation (Art. 6.1.c)	Per SEF/FINA requirements
Transactional email	email, invoice PDF	Contract (Art. 6.1.b)	Not stored by Bilko
Data export (portability)	All data	GDPR Art. 20 / ZZPL Art. 37	On demand

---

5. Data Flow Mapping

```
flowchart TD
    DS([Data Subject\nBusiness user]) -->|Registers / Creates invoice| COLLECT[Web App\nbilko.io — Vercel EU]
    COLLECT -->|HTTPS POST Zod validated| API[Express API\napi.bilko.io — Railway EU West]
    API -->|Prisma ORM AES-256| DB[(PostgreSQL\nRailway EU West\nFrankfurt/Paris)]
    API -->|Receipt upload| R2[(Cloudflare R2\nEU region AES-256)]
    DB -->|Append-only| AUDIT[(LoggedAction\nImmutable audit trail)]
    API -->|Invoice email| SG[SendGrid\nEU region]
    API -->|UBL 2.1 XML| SEF[SEF efaktura.gov.rs\nSerbia]
    API -->|UBL 2.1 HR-CIUS| FINA[HR-FISK fina.hr\nCroatia]
    DB -->|On deletion| ANON[Anonymization\nPII removed]
    DB -->|On export| EXPORT[JSON export to data subject]
    ANON --> DB

    style DB fill:#ffcccc,stroke:#cc0000
    style AUDIT fill:#ffe4cc,stroke:#cc6600
```

Data processors (GDPR Art. 28):

Processor	Service	Data Shared	Country	DPA Status
Railway	PostgreSQL hosting	All accounting data	EU West	Pending — sign before launch
Vercel	Frontend hosting	Browser requests	Global / EU edge	Pending
Cloudflare	CDN, WAF, R2	IP addresses, receipt files	EU region	Pending

Processor	Service	Data Shared	Country	DPA Status
SendGrid	Transactional email	Email, invoice PDFs	EU	Pending

6. Risk Assessment Matrix

6.1 Risk Scoring

Risk Score = Likelihood (1-5) × Severity (1-5). Score 1-6: Low; 7-12: Medium; 13-19: High; 20-25: Critical.

6.2 Risks to Data Subjects

Risk ID	Risk	Likelihood	Severity	Score	Controls	Residual
R1	Unauthorized access to financial data (tax IDs, IBAN, invoice amounts)	2	5	10	TLS 1.3, AES-256, RBAC, org-scoped queries	MEDIUM
R2	Tax ID (PIB/JMBG/OIB/JIB) theft enabling identity fraud	2	5	10	L4 Restricted, RBAC, no JWT exposure, bcrypt	MEDIUM
R3	Cross-tenant data access (IDOR)	2	5	10	org-scoped WHERE on all queries, UUID PKs	LOW (after mitigation)
R4	Invoice data exposure to wrong party	2	4	8	RBAC, org-scope, input validation	MEDIUM
R5	Financial data manipulation (tampered invoices)	2	5	10	Immutable LoggedAction, RBAC delete permissions	LOW (after mitigation)
R6	PII retained beyond necessary period	2	3	6	Soft delete + anonymization; financial data by law	LOW

Risk ID	Risk	Likelihood	Severity	Score	Controls	Residual
R7	Cross-border transfer (RS/BA data to EU) without protection	3	3	9	Railway EU West; ZZPL Art. 65; data stays in EEA	MEDIUM
R8	User unable to exercise erasure (locked by retention law)	3	2	6	Clear policy in privacy notice; PII anonymized	LOW
R9	Receipt with sensitive data (medical receipts) exposed	2	3	6	Encrypted R2 storage; RBAC accountant+ access	LOW
R10	Audit log IP retention enabling tracking	2	2	4	30-day IP retention for security; longer for financial	LOW
R11	SEF/HR-FISK state submission	1	2	2	Legal obligation — mandated by law	ACCEPTABLE

7. Mitigation Measures

Risk ID	Mitigation	Owner	Deadline	Status
R1	Field-level encryption for tax IDs and IBAN at application layer	Engineering	Phase 2	Planned
R1	Sentry error tracking + Railway anomaly monitoring	Platform	Phase 1	Planned
R2	Tax IDs L4 Restricted — never in JWT, never in logs	Engineering	Phase 1	Designed
R3	Integration tests: cross-tenant requests must return 403	Engineering	Phase 1	Planned
R4	Vitest RBAC tests on all protected endpoints	Engineering	Phase 1	Planned

Risk ID	Mitigation	Owner	Deadline	Status
R5	LoggedAction PostgreSQL trigger — append-only, no DELETE	Engineering	Phase 1	Designed
R7	Privacy notice states Railway EU West data residency; ZZPL Art. 65 transfer basis	Legal/DPO	Phase 1	Planned
R7	Verify Railway region = EU West before launch	Platform	Phase 1	Planned
R8	Privacy notice explains legal retention basis clearly	Legal/DPO	Phase 1	Planned
R9	R2 files accessible only to org members with accountant+ role	Engineering	Phase 1	Designed

Residual risk conclusion: All residual risks are LOW or MEDIUM. No CRITICAL or HIGH residual risks. Processing may proceed subject to DPO approval and Phase 1 mitigations being implemented before first paying customer.

DPO Conclusion: ☐ Acceptable — proceed | ☐ Conditional — pending Phase 1 mitigations | ☐ Escalate to supervisory authority

---

8. DPO Consultation Record

DPO Name: TBD (dpo@bilko.io) **Consultation Date:** To be scheduled before first paying customer

DPO Input:

> [To be completed after DPO appointment]

DPO Recommendation:

- ☐ Approved — risks acceptable and adequately mitigated
- ☐ Conditional approval — subject to Phase 1 mitigations

☐ Rejected — redesign required

☐ Escalate to supervisory authority

DPO Signature: _____ Date: _____

---

9. Supervisory Authority Consultation

Consultation Required: NO (pending DPO review) **Reason:** No CRITICAL or HIGH residual risks. MEDIUM risks standard for cloud accounting SaaS.

If required — relevant authorities by jurisdiction:

- HR: AZOP — azop@azop.hr — https://azop.hr
- RS: Poverenik — office@poverenik.rs — https://www.poverenik.rs
- BA: AZLP — info@azlp.ba — https://www.azlp.ba

---

10. DPIA Review Schedule

Next review: 2027-02-23 (annual) or when:

- New country launch (RS Phase 2, HR Phase 2, BA Phase 3)
- New government integration (SEF, HR-FISK, CPF)
- Data breach or near-miss
- New data categories or processors
- Regulatory changes (ZZPL amendment, BiH reform, GDPR updates)

Review Owner: DPO (dpo@bilko.io) **Review Log:**

Date	Reviewer	Changes	Outcome
2026-02-23	Compliance Architect	Initial DPIA	Draft — awaiting DPO

Approval

Role	Name	Date	Signature
Author	Compliance Architect	2026-02-23	
DPO			
Engineering Lead			

Role	Name	Date	Signature
Legal Counsel			
CEO			

Revision #9
Created 2026-02-23 12:02:57 UTC by John
Updated 2026-05-25 07:32:25 UTC by John