GDPR & Compliance

Bilko — Regulatory Compliance

Status: NOT COMPLIANT — Requires legal review and implementation (Phase 2)

This document outlines regulatory compliance requirements for Bilko as a Balkan accounting SaaS.

Compliance Scope

Bilko operates in a highly regulated space:

Region	Regulations
EU/EEA	GDPR (General Data Protection Regulation)
Serbia	Zakon o računovodstvu, SEF (Sistem E-Faktura)
Bosnia & Herzegovina	Zakon o PDV-u, Electronic bookkeeping requirements
Croatia	Zakon o fiskalizaciji, eRačun (public sector invoicing)

Current Status: MVP focuses on GDPR compliance. Balkan-specific regulations deferred to Phase 2.

Compliance Roadmap by Phase

```
graph LR
    subgraph P1["Phase 1 — MVP (pre-launch)"]
        GDPR["GDPR\nData minimization\nEncryption TLS+AES-256\nUser rights endpoints\nDPA with processors"]
    end

    subgraph P2["Phase 2 — Serbia Launch (3-6mo)"]
        RS_COA["Serbian CoA\n(Kontni plan template)"]
        RS_VAT["VAT 20%\nReporting"]
        RS_REP["Financial Reports\nBilans stanja\nBilans uspeha"]
```

```
        RS_SEF["SEF Integration\nB2G e-invoicing\n(optional at MVP)"]
    end

    subgraph P3["Phase 3 — Regional (12-18mo)"]
        BIH["BiH\nVAT 17%\nPDV prijava"]
        HR["Croatia\nVAT 25%\nFiskalizacija 2.0\neRačun B2G\nDigital signature"]
    end

    P1 --> P2 --> P3
```

GDPR (General Data Protection Regulation)

Applicability

- **Applies to:** All EU/EEA users (regardless of where Bilko is hosted)
- **Scope:** Personal data of natural persons (name, email, IP address)
- **Penalties:** Up to €20M or 4% of global turnover (whichever is higher)

Data We Collect

Data Type	Purpose	Legal Basis	Retention
Email	Account authentication	Contract performance	Until account deletion
Full name	User identification	Contract performance	Until account deletion
IP address	Security audit trail	Legitimate interest	30 days
Password (hashed)	Authentication	Contract performance	Until account deletion
Organization name	Service delivery	Contract performance	5 years (accounting law)
Financial records	Service delivery	Legal obligation	5-10 years (varies by country)

GDPR Principles Compliance

1. Lawfulness, Fairness, Transparency (Article 5(1)(a))

Implementation:

- Privacy policy visible before registration
- Terms of Service linked during signup
- Clear explanation of data usage
- No hidden data collection

Status: PLANNED — Privacy policy to be drafted

---

2. Purpose Limitation (Article 5(1)(b))

Implementation:

- Data used only for stated purposes (accounting, invoicing)
- No data selling to third parties
- No marketing emails without explicit consent

Status: COMPLIANT (by design)

---

3. Data Minimization (Article 5(1)(c))

Implementation:

- Only collect necessary data (email, name)
- No tracking cookies
- No analytics beyond server logs

Status: COMPLIANT (by design)

---

4. Accuracy (Article 5(1)(d))

Implementation:

- Users can update profile (email, name)
- Users can correct financial data (invoices, expenses)

Status: COMPLIANT (by design)

---

5. Storage Limitation (Article 5(1)(e))

Implementation:

- User data deleted on request (soft delete)
- Financial records retained 5 years (legal requirement overrides GDPR Article 17)
- Audit logs kept 30 days

Status: PLANNED — Deletion workflow to be implemented

---

6. Integrity & Confidentiality (Article 5(1)(f))

Implementation:

- TLS 1.3 encryption in transit
- AES-256 encryption at rest
- bcrypt password hashing
- Access controls (RBAC)

Status: PLANNED — See SECURITY-ARCHITECTURE.md

GDPR Data Flow Diagram

```
flowchart TD
    USER["User (Data Subject)"]
    REG["Registration\nPOST /api/v1/auth/register"]
    STORE_PII["Store PII\nRailway EU West (Frankfurt)\nAES-256 at rest\nemail, name, passwordHash (bcrypt)"]
    PROCESS["Service Processing\nInvoices, Expenses, Reports\nOrganization data"]
    LOG["Audit Trail\nLoggedAction table\nIP + timestamp (30 days)"]
    FILE["File Storage\nCloudflare R2 EU\nReceipts + PDFs\nAES-256"]

    subgraph THIRD["Third-Party Processors (DPA Required)"]
        RAILWAY["Railway EU West\n(DB hosting)"]
        VERCEL["Vercel\n(Frontend hosting)"]
        CF_R2["Cloudflare R2 EU\n(File storage)"]
        SG["SendGrid\n(Transactional email)"]
    end

    USER -->|"Consent via ToS"| REG --> STORE_PII
    STORE_PII --> PROCESS --> LOG
    PROCESS --> FILE

    STORE_PII --> RAILWAY
    REG --> VERCEL
    FILE --> CF_R2
    PROCESS -->|"Invoice emails"| SG
```

GDPR Rights (Articles 12-22)

Right to Access (Article 15)

User can request:

- Copy of all personal data
- Purpose of processing
- Data retention period

Implementation:

```
// Endpoint: GET /api/v1/account/data
await prisma.user.findUnique({
  where: { id: userId },
  include: { organization: true, auditLogs: true },
});
```

Status: PLANNED

Right to Rectification (Article 16)

User can:

- Update email, name
- Correct invoices, expenses

Implementation:

```
// Endpoint: PATCH /api/v1/account/profile
await prisma.user.update({
  where: { id: userId },
  data: { email, fullName },
});
```

Status: PLANNED

Right to Erasure (Article 17)

Exceptions:

- Financial records must be kept 5 years (legal obligation overrides)
- Audit logs anonymized (user ID replaced with "deleted-user")

Implementation:

```
// Endpoint: DELETE /api/v1/account
await prisma.user.update({
  where: { id: userId },
  data: {
    email: `deleted-${userId}@example.com`,
    fullName: 'Deleted User',
    passwordHash: '',
    deletedAt: new Date(),
  },
});
```

Status: PLANNED

Right to Data Portability (Article 20)

User can:

- Export all data in JSON format

Implementation:

```
// Endpoint: GET /api/v1/account/export
const data = {
  user: await prisma.user.findUnique({ where: { id: userId } }),
  invoices: await prisma.invoice.findMany({ where: { organizationId } }),
  expenses: await prisma.expense.findMany({ where: { organizationId } }),
};
res.json(data);
```

Status: PLANNED

Right to Object (Article 21)

Not applicable — Bilko does not use profiling or automated decision-making.

Data Processing Agreement (DPA)

Required when Bilko processes customer data on behalf of organizations.

Third-Party Processors:

Service	Purpose	DPA Available?	GDPR Compliant?
Railway	Database hosting	Yes	Yes (EU region)
Vercel	Frontend hosting	Yes	Yes
Cloudflare	R2 storage, DNS	Yes	Yes
SendGrid	Transactional email	Yes	Yes

Action Required: Sign DPAs with all processors before launch.

Status: PENDING

Data Breach Notification (Article 33)

Requirement:

- Notify supervisory authority within 72 hours of breach
- Notify affected users if high risk to rights and freedoms

Process:

1. Detect breach (monitoring, user report)
2. Assess impact (how many users, what data)
3. Contain breach (block attacker, revoke tokens)
4. Notify authority (within 72h)
5. Notify users (if high risk)
6. Document incident (post-mortem)

Breach Notification Flow

```
sequenceDiagram
    participant MON as Monitoring (Sentry / Railway)
    participant JOHN as John (AI Director)
    participant ALEM as Alem (CEO)
    participant AUTH as Supervisory Authority
    participant USERS as Affected Users

    MON->>JOHN: Alert: anomaly detected
    JOHN->>JOHN: Assess impact\n(data type, user count)
    JOHN->>JOHN: Contain: revoke tokens\nblock attacker IP
```

```
    JOHN->>ALEM: Breach report + impact summary

    alt High risk to users
        ALEM->>AUTH: Notify within 72h (GDPR Art. 33)
        ALEM->>USERS: Email notification\n(nature of breach, data affected,\nsteps taken)
    else Low risk
        ALEM->>AUTH: Optional notification
        Note over USERS: No user notification required
    end

    JOHN->>JOHN: Post-mortem\nUpdate security docs\nPatch vulnerability
```

Status: PLANNED — Incident response plan documented in SECURITY-ARCHITECTURE.md

---

Data Protection Officer (DPO)

Required? No — Bilko does not meet GDPR Article 37 criteria:

- Not a public authority
- Not large-scale systematic monitoring
- Not large-scale processing of sensitive data

Threshold: DPO required if >250 employees or large-scale processing. Bilko is small startup.

Status: NOT REQUIRED (as of 2026-02-20)

Data Residency

Requirement: Store EU user data within EU/EEA (GDPR Article 44-50)

Implementation:

- Railway: EU West region (Frankfurt or Paris)
- Vercel: Edge network (serves from EU for EU users)
- Cloudflare R2: EU region

Status: PLANNED — Configure Railway to EU region on deployment

---

Serbia — Zakon o ra?unovodstvu (Accounting Law)

Applicability

- **Applies to:** All legal entities in Serbia
- **Scope:** Financial record-keeping, reporting, retention

Requirements

1. Chart of Accounts

Regulation: Companies must use standardized chart of accounts (Kontni plan)

Implementation:

- Bilko allows custom chart of accounts
- Provide Serbian CoA template (predefined accounts)

Status: PLANNED — Create Serbian CoA seed data

---

2. Double-Entry Bookkeeping

Regulation: All transactions must use double-entry (debit + credit)

Implementation:

- Prisma schema enforces double-entry (`debitAccountId` + `creditAccountId`)
- Backend validates debit = credit

Status: COMPLIANT (by design)

---

3. Financial Reporting

Required reports:

- Bilans stanja (Balance Sheet)
- Bilans uspeha (Income Statement)
- Izvještaj o novčanim tokovima (Cash Flow Statement)

Implementation:

- Bilko generates P&L, Balance Sheet, Cash Flow
- Export to PDF (Serbian language support)

Status: PLANNED — Backend report generation

---

4. Data Retention

Regulation: Financial records must be kept minimum 5 years

Implementation:

- Soft delete (never hard delete financial data)
- Backup retention: 30 days (Railway automatic backups)

Status: PLANNED

SEF (Sistem E-Faktura) — Electronic Invoicing

Requirement: B2G (business-to-government) invoices must be submitted electronically via SEF portal.

Applicability:

- Mandatory for government contracts
- Optional for B2B (as of 2026)

Implementation (Phase 2):

- SEF XML export format
- API integration with SEF portal
- Digital signature (qualified certificate)

Status: NOT IMPLEMENTED — Deferred to Phase 2

Bosnia & Herzegovina — Zakon o PDV-u (VAT Law)

VAT Rates

- **Standard:** 17%
- **Reduced:** 0% (exports, specific goods)

Requirements

1. VAT Calculation

Implementation:

- Bilko supports configurable tax rates per invoice item
- Default tax rate: 17% for BiH organizations

Status: COMPLIANT (by design)

---

2. VAT Reporting

Required report:

- PDV prijava (VAT return) — monthly or quarterly

Implementation:

- Bilko generates VAT report (sales, purchases, net VAT)
- Export to PDF

Status: PLANNED — Backend report generation

---

3. Electronic Bookkeeping

Regulation: Companies with revenue >50,000 BAM must maintain electronic records.

Implementation:

- Bilko is cloud-based (electronic by default)
- Data export to XML (future integration with tax authority)

Status: PLANNED (Phase 2)

Croatia — Zakon o fiskalizaciji (Fiscalization Law)

Applicability

- **Applies to:** All businesses with cash transactions (retail, hospitality, services)

Requirements

1. Fiscalization (Fiskalizacija 2.0)

Regulation: All invoices must be registered with tax authority in real-time.

Implementation (Phase 2):

- API integration with Porezna uprava (tax authority)
- Digital signature (qualified certificate)
- Unique invoice identifier (JIR) from tax authority
- QR code on invoice (links to tax authority verification)

Status: NOT IMPLEMENTED — Deferred to Phase 2

---

2. eRa?un (Public Sector Invoicing)

Requirement: B2G invoices must be submitted via eRačun system.

Implementation (Phase 2):

- UBL XML format
- Integration with eRačun portal

Status: NOT IMPLEMENTED — Deferred to Phase 2

Multi-Country Compliance Matrix

Requirement	Serbia	BiH	Croatia	Implementation Status
Double-entry bookkeeping	Required	Required	Required	Compliant (Prisma schema)
VAT calculation	20%	17%	25%	Compliant (configurable)
VAT reporting	Required	Required	Required	Planned
Financial reports	Required	Required	Required	Planned

Requirement	Serbia	BiH	Croatia	Implementation Status
Data retention (5 years)	Required	Required	Required	Planned
Electronic invoicing (B2G)	SEF	Optional	eRačun	Phase 2
Real-time fiscalization	Not required	Not required	Required	Phase 2
Digital signature	Not required	Not required	Required	Phase 2

Data Retention Lifecycle

```
stateDiagram-v2
    [*] --> Active : User registers

    Active --> DeletionRequested : POST /api/v1/account/delete
    Active --> Active : Normal usage\n(invoices, expenses, reports)

    DeletionRequested --> SoftDeleted : Anonymize PII\nemail → deleted-
{uuid}@example.com\nname → "Deleted User"\npasswordHash → ""

    SoftDeleted --> AuditAnonymized : Replace userId\nin LoggedAction\nwith "deleted-user"

    AuditAnonymized --> FinancialRetained : Financial records\nKEPT for 5 years\n(legal
obligation Serbia/BiH/HR)

    FinancialRetained --> PermanentDelete : After 5-year\nretention period

    PermanentDelete --> [*]

    note right of Active
        IP logs: 30 days
        Audit trail: 30 days
        Financial data: indefinite (legal)
    end note

    note right of FinancialRetained
```

```
        Invoices, expenses,\ntransactions, reports\nretained per Zakon o računovodstvu
        User PII already anonymized
    end note
```

Compliance Roadmap

Phase 1 (MVP) — GDPR Only

- ☐ Privacy policy drafted
- ☐ Terms of Service drafted
- ☐ Data minimization (by design)
- ☐ Encryption (TLS + AES-256)
- ☐ User data deletion workflow
- ☐ Data export (JSON)
- ☐ Sign DPAs with processors

Timeline: Pre-launch (before first customer)

Phase 2 (Serbia Launch)

- ☐ Serbian CoA template
- ☐ VAT reporting (20%)
- ☐ Financial reports (Balance Sheet, P&L, Cash Flow)
- ☐ SEF integration (B2G invoicing)
- ☐ Legal review by Serbian lawyer

Timeline: 3-6 months after MVP

Phase 3 (Regional Expansion)

- ☐ BiH VAT support (17%)
- ☐ Croatian VAT support (25%)
- ☐ Croatian fiscalization (real-time)
- ☐ eRačun integration (Croatia)
- ☐ Multi-language support (SR, BS, HR)

Timeline: 12-18 months after MVP

Compliance Checklist (Pre-Launch)

GDPR

- ☐ Privacy policy published
- ☐ Terms of Service published
- ☐ Cookie banner (if using cookies)
- ☐ User consent mechanism
- ☐ Data deletion workflow
- ☐ Data export endpoint
- ☐ DPAs signed (Railway, Vercel, Cloudflare, SendGrid)
- ☐ Railway EU region configured
- ☐ Breach notification process documented

Serbia (Phase 2)

- ☐ Legal review (Serbian accounting law)
- ☐ Serbian CoA template
- ☐ VAT calculation (20%)
- ☐ Financial reports (Serbian format)
- ☐ SEF integration (optional for MVP)

BiH (Phase 3)

- ☐ Legal review (BiH VAT law)
- ☐ VAT calculation (17%)
- ☐ PDV prijava report

Croatia (Phase 3)

- ☐ Legal review (Croatian fiscalization law)
- ☐ VAT calculation (25%)
- ☐ Fiscalization integration (mandatory)
- ☐ Qualified digital certificate
- ☐ eRačun integration

Risk Assessment

Risk	Likelihood	Impact	Mitigation
GDPR fine	Low (if compliant)	High (€20M)	Implement all GDPR requirements pre-launch
Data breach	Medium	High	Encryption, rate limiting, security audit
Serbian non-compliance	Medium	Medium	Hire local accountant as advisor
Croatian fiscalization failure	Low (Phase 3)	High	Partner with Croatian accounting firm
User data loss	Low	High	Daily backups, test restore process

Legal Disclaimer

IMPORTANT: This document is for internal planning only. It is NOT legal advice.

Before launch:

- Consult GDPR lawyer (EU compliance)
- Consult Serbian lawyer (accounting law)
- Consult BiH/Croatian lawyers (Phase 2/3)
- Review Privacy Policy with lawyer
- Review Terms of Service with lawyer

Recommended Lawyers:

- GDPR: Find lawyer specialized in EU data protection
- Serbia: Find lawyer specialized in računovodstvo (accounting law)

Related Documents

- Security Architecture: SECURITY-ARCHITECTURE.md
- Deployment Guide: ../infrastructure/DEPLOYMENT.md
- Privacy Policy: Privacy Policy *(not yet created)* (to be created)

- Terms of Service: Terms of Service *(not yet created)* (to be created)

Last Updated: 2026-02-20 **Status:** NOT COMPLIANT — Requires implementation and legal review **Next Review:** Before first paying customer **Compliance Officer:** TBD (hire accounting advisor in Phase 2)

Revision #5
Created 2026-02-23 10:48:11 UTC by John
Updated 2026-05-31 20:02:49 UTC by John