

Compliance Overview

Bilko — Regulatory Compliance

“ **Project:** Bilko **Version:** 1.0 **Date:** 2026-02-25 **Author:** ALAI Documentation Team **Status:** Final **Note:** Compliance implementation status is tracked per jurisdiction below. Document is finalized for Phase 1 MVP scope.

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.

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 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

Service	Purpose	DPA Available?	GDPR Compliant?
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)

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

Balkan Data Protection Laws

Regulatory Comparison: RS / BA / HR

Dimension	Serbia (RS)	Bosnia & Herzegovina (BA)	Croatia (HR)
Law	ZZPL — Zakon o zaštiti podataka o ličnosti (Sl. glasnik RS 87/2018)	ZZLP BiH — Zakon o zaštiti ličnih podataka (Sl. glasnik BiH 49/2006)	GDPR — Uredba (EU) 2016/679 (directly applicable)
Model	GDPR-aligned (adopted 2018, effective 2019)	Pre-GDPR, older framework (2006)	Full EU GDPR — identical to GDPR
Supervisory Authority	Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti	Agencija za zaštitu ličnih podataka (AZLP)	Agencija za zaštitu osobnih podataka (AZOP)
Authority Website	poverenik.rs	azlp.gov.ba	azop.hr
Notification Email	poverenik@poverenik.rs	azlp@azlp.gov.ba	azop@azop.hr
Max Penalty (legal entity)	2,000,000 RSD (~€17,000)	10,000 BAM (~€5,000)	€20,000,000 or 4% global annual turnover
Breach notification deadline	72 hours (ZZPL Art. 56 — GDPR Art. 33 equivalent)	Best practice 72 hours (ZZLP BiH less specific)	72 hours (GDPR Art. 33)
DPO Required?	No (same thresholds as GDPR Art. 37)	No mandatory DPO provision	No (same thresholds as GDPR Art. 37)
Legal basis for processing	Art. 12 ZZPL (mirrors GDPR Art. 6)	Art. 5 ZZLP BiH	GDPR Art. 6 directly

Serbia ZZPL — Key Differences from GDPR

- **Article equivalences:** ZZPL Art. 26 = GDPR Art. 15 (access), Art. 27 = Art. 16 (rectification), Art. 28 = Art. 17 (erasure), Art. 30 = Art. 20 (portability)

- **Registration:** No requirement to register with Poverenik for standard processing (registration abolished in ZZPL 2018 reform)
- **Transfers:** Serbia recognized as adequate jurisdiction by European Commission (Decision 2023/1485 of July 21, 2023) — data can flow RS ↔ EU without additional mechanisms
- **Enforcement:** Poverenik has investigative and corrective powers; administrative fines up to 2M RSD; criminal liability for intentional violations

BiH ZZLP — Key Differences from GDPR

- **Entity structure:** BiH has two entities (FBiH and RS entity) plus Brčko District — ZZLP BiH applies at state level, but FBiH and RS entity have their own accounting laws
- **Older law:** ZZLP BiH dates from 2006 — less specific on breach notification timing, no explicit DPO requirement, narrower data subject rights
- **No adequacy decision:** BiH is NOT on EU adequacy list. Cross-border transfers from BiH users to EU-hosted infrastructure require Standard Contractual Clauses (SCCs 2021/914)
- **AZLP powers:** Lower penalty ceiling (10K BAM) but can prohibit processing as sanction
- **Practical note:** BiH law reform expected ~2026-2027 to align with GDPR — monitor for updates

Croatia GDPR — Implementation Notes

- **Full GDPR:** Croatia is EU member — GDPR applies directly since 2018. No separate Croatian data protection law needed
- **AZOP:** Croatian DPA; can issue fines up to €20M or 4% global turnover
- **Supplementing law:** Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18) — national provisions for derogations (e.g., age of consent 16 years for online services)
- **HR-specific requirement:** Croatian law requires data processing records (čl. 30 GDPR) maintained in Croatian if requested by AZOP

Data Retention Policy by Jurisdiction

Retention Requirements — Financial & Accounting Records

Data Category	Serbia (RS)	BiH — FBiH	BiH — RS Entity	Croatia (HR)	Legal Basis
---------------	-------------	------------	-----------------	--------------	-------------

Financial statements	10 years	10 years	10 years	11 years	RS: Zakon o računovodstvu Art. 26; BA FBiH: Art. 17; BA RS: Art. 16; HR: Zakon o računovodstvu Art. 10
Invoices (issued & received)	10 years	10 years	10 years	11 years	Same as above
Bank account statements	10 years	10 years	10 years	11 years	Same as above + Opći porezni zakon (HR)
Tax returns (VAT, CIT)	10 years	10 years	10 years	11 years	RS: Zakon o porezu na dodatu vrednost; HR: Opći porezni zakon Art. 92
Employee payroll records	10 years	10 years	10 years	11 years	Mandatory for pension/social security compliance
Expense receipts	10 years	10 years	10 years	11 years	Same as invoices
Audit trail (LoggedAction)	10 years	10 years	10 years	11 years	Derived from financial record retention

Retention Requirements — Personal Data (GDPR/ZZPL/ZZLP)

Data Category	Retention Period	Legal Basis
User email, name	Account lifetime + 30 days after deletion	Contract performance (GDPR Art. 6(1)(b))
IP addresses, session logs	30 days	Legitimate interest (security) — minimal period
Tax IDs (PIB, JMBG, OIB, JIB)	10–11 years	Legal obligation — accounting/tax law overrides GDPR Art. 17(3)(b)
IBAN numbers	10–11 years	Legal obligation — same override
Backup copies	Railway: 7-day automatic backup window	Technical necessity

Data Category	Retention Period	Legal Basis
Deleted user account data	30 days after soft delete (then hard delete PII)	Minimize retention per GDPR Art. 5(1)(e)

Retention Enforcement in Bilko

```
// Delete-prevention lock – prevents hard delete during mandatory retention period
async function canDeleteFinancialRecord(recordId: string, createdAt: Date): Promise<boolean> {
  const jurisdiction = await getOrganizationJurisdiction(recordId)
  const retentionYears = jurisdiction === 'HR' ? 11 : 10 // BA RS entity is 11 too
  const cutoffDate = new Date()
  cutoffDate.setFullYear(cutoffDate.getFullYear() - retentionYears)

  if (createdAt > cutoffDate) {
    throw new Error(
      `Financial record cannot be deleted: retention period (${retentionYears} years) not
elapsed`,
    )
  }
  return true
}
```

Data Residency Requirements

Primary Infrastructure

All Bilko production data is hosted in **Railway EU West** (Amsterdam or Frankfurt):

- **PostgreSQL database:** Railway EU West — encrypted at rest (AES-256)
- **File storage:** Cloudflare R2, EU region (Amsterdam)
- **CDN / WAF:** Cloudflare EU edge nodes serve EU users first
- **Error tracking:** Sentry (EU region SaaS) — configured for EU data residency

Jurisdiction-Specific Requirements

Jurisdiction	Data Residency Law	Requirement	Bilko Implementation
--------------	--------------------	-------------	----------------------

Croatia (HR)	GDPR Art. 44-50	EU/EEA storage for personal data	Railway EU West ☐
Serbia (RS)	ZZPL Art. 64-70	No mandatory localization; adequacy decision covers RS↔EU transfers	Railway EU West ☐ (adequacy covers this)
Bosnia & Herzegovina (BA)	ZZLP BiH Art. 14-17	No explicit localization law; SCC required for EU transfers	Railway EU West + SCC with Railway ☐

Configuration Checklist

- ☐ Railway project region set to EU West (Amsterdam) before first deployment
- ☐ Cloudflare R2 bucket created in EU region (`EEUR` or `WEUR`)
- ☐ Sentry project set to EU data region (app.eu.sentry.io)
- ☐ All DATABASE_URL connection strings use Railway EU West endpoint

Cross-Border Data Transfer Rules

Transfer Mechanism Summary

Data Flow	Transfer Type	Legal Mechanism	Required Action
HR users → Railway EU West	EU → EU (intra-EEA)	No mechanism needed	None
RS users → Railway EU West	Third country → EU	EU Adequacy Decision 2023/1485 (Serbia)	No additional contracts needed
BA users → Railway EU West	Third country → EU	No adequacy decision for BiH	Standard Contractual Clauses (SCCs 2021/914) required
API → Sentry (error tracking)	EU → EU	Sentry EU region	Configure Sentry EU DSN
API → SEF portal (Serbia)	EU host → RS gov portal	RS domestic processing	No GDPR concern (processed in RS by RS authority)
API → FINA/HR-FISK (Croatia)	EU → EU	EU to EU	No mechanism needed

Standard Contractual Clauses — BiH Users

For BiH users whose data is stored on Railway (EU host):

1. **Module 2 SCCs** (Controller-to-Processor) required: Bilko as controller → Railway as processor
2. **Railway DPA** includes SCCs 2021/914 for non-EEA transfers
3. **Transfer Impact Assessment (TIA)** required before relying on SCCs:
 - Railway is US company but data stored in EU — assess EU GDPR applicability
 - Cloudflare processes BiH IP addresses at edge — assess data minimization
4. **Action required:** Sign Railway DPA with SCC addendum before accepting BiH customers

Serbia Adequacy Decision

- **Decision:** European Commission Implementing Decision 2023/1485 of July 21, 2023
- **Effect:** Serbia treated as providing adequate protection equivalent to EU GDPR
- **Practical:** No SCCs, BCRs, or other transfer mechanisms needed for RS↔EU data flows
- **Caveat:** Adequacy decisions can be revoked — monitor European Commission communications

BiH Adequacy Status

- **Current status:** BiH does NOT have EU adequacy decision (as of 2026)
 - **Expected:** ZZLP reform expected ~2027 may trigger adequacy assessment
 - **Action:** Track EDPB opinions and European Commission decisions for BiH
-

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)
- Izveštaj 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. eRačun (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
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

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

Risk	Likelihood	Impact	Mitigation
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: [../legal/PRIVACY-POLICY.md](#)
- Terms of Service: [../legal/TERMS-OF-SERVICE.md](#)

Last Updated: 2026-02-25 **Status:** Final **Compliance Implementation:** In Progress — GDPR Phase 1 pre-launch; Balkan regulations Phase 2 **Next Review:** Before first paying customer **Compliance Officer:** Deferred to Phase 2 — accounting advisor to be engaged before Serbia launch