Compliance Framework

Compliance Framework Document

> **Project:** Bilko — Balkan Accounting SaaS **Version:** 1.0 **Date:** 2026-02-23 **Author:** Compliance Architect **Status:** Draft **Reviewers:** DPO, Legal Counsel, CEO **Classification:** Confidential

Document History

Version	Date	Author	Changes
0.1	2026-02-23	Compliance Architect	Initial draft — RS/BA/HR three-country compliance mapping

---

1. Applicable Regulations

Compliance Owner: Compliance Architect (compliance@bilko.io) **Last Review:** 2026-02-23 | **Next Review:** 2026-08-23

Regulation	Country	Phase
GDPR — Regulation (EU) 2016/679	HR	Phase 1
Zakon o zaštiti podataka o ličnosti (ZZPL, Sl. glasnik RS 87/2018)	RS	Phase 2
Zakon o zaštiti ličnih podataka BiH (ZZLP, Sl. glasnik BiH 49/2006)	BA	Phase 3
Zakon o računovodstvu (Sl. glasnik RS 73/2019)	RS	Phase 2

Regulation	Country	Phase
Zakon o računovodstvu i reviziji FBiH (Sl. novine FBiH 83/2009)	BA (FBiH)	Phase 3
Zakon o računovodstvu i reviziji RS BiH (Sl. glasnik RS BiH 96/2005)	BA (RS entity)	Phase 3
Zakon o računovodstvu HR (NN 78/15, 120/16, 116/18)	HR	Phase 2
Zakon o PDV RS (Sl. glasnik RS 84/2004 et al.)	RS	Phase 2
Zakon o PDV BiH (Sl. glasnik BiH 9/2005 et al.)	BA	Phase 3
Zakon o porezu na dodanu vrijednost HR (NN 73/13 et al.)	HR	Phase 2
Zakon o elektronskom dokumentu RS (Sl. glasnik RS 51/2009)	RS	Phase 2
Opći porezni zakon HR (NN 115/16 et al.)	HR	Phase 2
Pravilnik o kontnom okviru RS (2021)	RS	Phase 2
FBiH Pravilnik o kontnom okviru (2022)	BA (FBiH)	Phase 3
RRiF Kontni plan HR	HR	Phase 2

2. Serbia (RS) — Regulatory Compliance

2.1 Data Protection — Zakon o zaštiti podataka o li?nosti (ZZPL)

Full name: Zakon o zaštiti podataka o ličnosti **Citation:** Sl. glasnik RS br. 87/2018 **In force:** November 21, 2018 **Description:** Serbia's GDPR-aligned personal data protection law. **Supervisory authority:** Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti **Website:** https://www.poverenik.rs

Requirement	ZZPL Article	Bilko Implementation
Lawful basis for processing	Art. 12	Contract (Art. 12 st. 1 tač. 2) — accounting service

Requirement	ZZPL Article	Bilko Implementation
Data minimization	Art. 5 st. 1 tač. 3	Email, name, PIB/JMBG only where legally required
Data subject rights	Art. 26-41	GET /account/data, DELETE /account, GET /account/export
Processing register	Art. 50	Internal processing register required
Security of processing	Art. 50	TLS 1.3, AES-256, bcrypt, RBAC
Breach notification to Poverenik	Art. 56	Within 72 hours of awareness

Breach notification: office@poverenik.rs | Bulevar kralja Aleksandra 15, 11000 Belgrade

2.2 Accounting Law — Zakon o ra?unovodstvu

Full name: Zakon o računovodstvu **Citation:** Sl. glasnik RS br. 73/2019, 44/2021

Requirement	Bilko Implementation
Double-entry bookkeeping	Schema enforces debitAccountId + creditAccountId
Chart of accounts: Pravilnik o kontnom okviru (2021) — 10 class (0-9)	Serbian CoA seed data
Bilans stanja (Balance Sheet) + Bilans uspeha (Income Statement)	Phase 2 reports
Filing: APR (https://www.apr.gov.rs), deadline June 30	PDF export + reminders
Document retention: **10 years**	Soft delete — never hard delete financial data

2.3 VAT — Zakon o PDV

Citation: Sl. glasnik RS br. 84/2004 (consolidated)

Rate	Description
20% (opšta stopa)	Standard — general goods and services
10% (snižena stopa)	Reduced — food, medicines, utilities
0%	Exports, international transport

VAT threshold: 8,000,000 RSD | **Return:** Monthly (>50M RSD) or Quarterly | **Deadline:** 15th of next month

2.4 E-Invoice — SEF (Sistem e-Faktura)

Platform: https://efaktura.gov.rs | **Mandatory:** B2B since January 2023 **Format:** UBL 2.1 XML | **Penalties:** 50,000–2,000,000 RSD for non-compliance **Integration:** `@bilko/country-rs` package (Phase 2)

2.5 APR Filing

Serbian entities file annual financial reports with APR (Agencija za privredne registre). Deadline: June 30. Bilko generates APR-compatible PDF/XML exports.

---

3. Bosnia & Herzegovina (BA) — Regulatory Compliance

Complexity: BiH has two entities (FBiH and Republika Srpska). VAT unified at state level via UIO. Direct taxes separate per entity.

3.1 Data Protection — Zakon o zaštiti li?nih podataka BiH (ZZLP)

Full name: Zakon o zaštiti ličnih podataka Bosne i Hercegovine **Citation:** Sl. glasnik BiH br. 49/2006, 76/2011, 89/2011 **Supervisory authority:** AZLP — Agencija za zaštitu ličnih podataka Bosne i Hercegovine **Website:** https://www.azlp.ba

Requirement	ZZLP Article	Bilko Implementation
Lawful basis	Art. 4	Contract + legal obligation
Security measures	Art. 14	TLS 1.3, AES-256, bcrypt, RBAC
Cross-border transfer	Art. 18	Railway EU West — SCCs mechanism
Breach notification to AZLP	Art. 14 + GDPR practice	72 hours

Breach notification: info@azlp.ba | Hamdije Čemerlića 2/VI, 71000 Sarajevo

3.2 FBiH — Accounting Law

Full name: Zakon o računovodstvu i reviziji Federacije Bosne i Hercegovine **Citation:** Sl. novine FBiH br. 83/2009, 56/2023

Requirement	Bilko Implementation

Double-entry bookkeeping	Schema enforced
Chart of accounts: FBiH Pravilnik (2022)	BiH CoA seed data
Filing: Agency of Financial Information (FBiH), deadline March 31	PDF export
Document retention: **10 years**	Immutable storage

3.3 Republika Srpska (BA Entity)

Citation: Sl. glasnik RS BiH br. 96/2005, 74/2016 **Filing:** Tax Administration of RS (BiH entity), March 31 **Retention: 11 years** — maximum applied across BA entities

3.4 VAT — Zakon o PDV BiH

Citation: Sl. glasnik BiH br. 9/2005 (consolidated) **Authority:** UIO — Uprava za indirektno oporezivanje | https://www.uino.gov.ba

Rate	Description
17% (opća stopa)	Standard — all goods and services
0%	Exports

Threshold: 100,000 BAM | **Return:** Monthly | **No reduced rates**

3.5 E-Invoice — CPF (Central Platform for Fiscalisation)

Status: PENDING — technical specifications not published **Law adopted:** January 2026 (FBiH only) **Expected:** ~2027

Bilko decision: DO NOT implement CPF until specs published. BiH is Phase 3 launch.

3.6 Corporate Income Tax

Entity	Rate	Deadline
FBiH	10%	March 31
RS (BiH entity)	10%	March 31

4. Croatia (HR) — Regulatory Compliance

Note: Croatia is EU member state. GDPR applies directly.

4.1 Data Protection — GDPR

Applicable: GDPR Regulation (EU) 2016/679 (directly applicable) **National implementing act:** Zakon o provedbi Opće uredbe (NN 42/2018) **Supervisory authority:** AZOP — Agencija za zaštitu osobnih podataka | https://azop.hr

Requirement	GDPR Article	Bilko Implementation
Lawful basis	Art. 6	Contract (6.1.b) for service; legal obligation (6.1.c) for tax
Data minimization	Art. 5(1)(c)	OIB, name, email only
Right to access	Art. 15	GET /api/v1/account/data
Right to erasure	Art. 17	DELETE /api/v1/account
Right to portability	Art. 20	GET /api/v1/account/export
Security of processing	Art. 32	TLS 1.3, AES-256, bcrypt, RBAC
Breach notification to AZOP	Art. 33	Within 72 hours
DPA with processors	Art. 28	Railway, Vercel, Cloudflare, SendGrid

Breach notification: azop@azop.hr | https://azop.hr/prijavapovrede | Selska cesta 136, 10000 Zagreb

4.2 Accounting Law — Zakon o ra?unovodstvu HR

Citation: NN 78/15, 120/16, 116/18, 42/20

Requirement	Bilko Implementation
Double-entry bookkeeping	Schema enforced
Chart of accounts: RRiF standard	HR CoA seed data
Accounting standards: CFRS (SMEs) or IFRS (PIEs)	CFRS-compliant reports
Bilanca + Račun dobiti i gubitka	Report generation Phase 2
Filing: FINA RGFI (https://www.fina.hr), deadline April 30	FINA-compatible export

Requirement	Bilko Implementation
Document retention: **11 years**	Immutable storage

4.3 General Tax Law — Op?i porezni zakon HR

Citation: NN 115/16, 106/18, 121/19, 32/20 Document retention 11 years, electronic record acceptance, digital accounting system obligations.

4.4 VAT — Zakon o PDV HR

Citation: NN 73/13 et al. | **Portal:** ePorezna — https://www.porezna-uprava.hr

Rate	Description
25% (opća stopa)	Standard — general goods and services
13% (srednja stopa)	Intermediate — foods, water, accommodation
5% (snižena stopa)	Reduced — books, baby food, medicines
0%	Exports, intra-EU supply

Threshold: 60,000 EUR | **Return:** Monthly | **Deadline:** Last day of next month

4.5 E-Invoice — HR-FISK / eRa?un

Platform: https://hr-fisk.fina.hr | **Operator:** FINA — Financijska agencija **Mandatory since:** January 1, 2026 (all B2B, B2G, B2C) **Format:** UBL 2.1 XML with HR-CIUS | **Protocol:** AS4 (Peppol-compatible) **Certificate:** FINA qualified certificate required **Penalties:** Up to EUR 500,000 for non-compliance **Archive:** 11 years

Integration: `@bilko/country-hr` — FINA certificate + API (Phase 2)

4.6 Corporate Income Tax — Croatia

- Standard rate: 18% | Reduced: 10% (revenue <1M EUR) | Deadline: April 30

---

5. Cross-Country Compliance Matrix

Requirement	Serbia (RS)	Bosnia & Herzegovina (BA)	Croatia (HR)
Data protection law	ZZPL (GDPR-aligned, 2018)	ZZLP BiH (2006)	GDPR (directly applicable)

Requirement	Serbia (RS)	Bosnia & Herzegovina (BA)	Croatia (HR)
Supervisory authority	Poverenik	AZLP	AZOP
Breach notification deadline	72 hours (ZZPL Art. 56)	72 hours (best practice)	72 hours (GDPR Art. 33)
VAT standard rate	20%	17%	25%
VAT reduced rate	10%	None	13% / 5%
E-invoice platform	SEF (mandatory Jan 2023)	CPF (pending ~2027)	HR-FISK (mandatory Jan 2026)
E-invoice format	UBL 2.1 XML	TBD	UBL 2.1 XML (HR-CIUS)
Annual report filing	APR — June 30	Agency Fin. Info / Tax Admin — March 31	FINA RGFI — April 30
Chart of accounts	Pravilnik (2021)	FBiH Pravilnik (2022)	RRiF standard
Document retention	**10 years**	**10 (FBiH) / 11 (RS entity)**	**11 years**
Currency	RSD	BAM	EUR
CIT rate	15%	10%	18% (10% <1M EUR)

Bilko retention policy: Apply maximum across all markets — **11 years** for all financial records. Never hard delete.

---

6. Data Classification Scheme

Level	Label	Examples	Controls
L1	Public	Exchange rates, fee schedule, privacy policy	None
L2	Internal	Aggregated analytics, non-PII logs	Access control
L3	Confidential	Email, name, organization data, invoice amounts	Encryption + access control + audit
L4	Restricted	PIB/JMBG/OIB/JIB (tax IDs), IBAN, TOTP secrets, password hashes	Encryption + RBAC + MFA + audit + 11-year retention

Tax ID types by country:

- Serbia: PIB (9 digits), JMBG (13 digits)
- BiH: JIB (13 digits)
- Croatia: OIB (11 digits)

7. Data Subject Rights Implementation

Right	Endpoint	SLA	Exception
Access (GDPR Art. 15 / ZZPL Art. 26)	GET /api/v1/account/data	30 days	—
Rectification (Art. 16)	PATCH /api/v1/account/profile	Immediate	—
Erasure (Art. 17)	DELETE /api/v1/account	30 days	Financial records retained per law
Portability (Art. 20)	GET /api/v1/account/export	30 days	—
Restriction (Art. 18)	compliance@bilko.io	30 days	Manual

Erasure exception: Invoices, expenses, transactions retained 10-11 years (accounting law). Only PII (email, name, password hash) anonymized.

8. Third-Party Data Processors

Processor	Service	Region	DPA Status
Railway	PostgreSQL hosting	EU West (Frankfurt/Paris)	Required — sign before launch
Vercel	Frontend hosting	EU edge	Required
Cloudflare	CDN, WAF, R2 storage	EU region	Required
SendGrid	Transactional email	EU	Required

9. Compliance Roadmap

Phase 1 — Pre-Launch (GDPR baseline)

- ☐ Privacy policy published
- ☐ Terms of Service published
- ☐ User consent mechanism at registration
- ☐ Data deletion + anonymization workflow

- [ ] Data export endpoint
- [ ] DPAs signed: Railway, Vercel, Cloudflare, SendGrid
- [ ] Railway EU West region confirmed
- [ ] Breach notification process ready

Phase 2 — Serbia Launch + Croatia Launch

Serbia:

- [ ] Legal review (accounting law + ZZPL)
- [ ] Serbian CoA seed data (Pravilnik 2021)
- [ ] VAT at 20% / 10%
- [ ] SEF XML export + API integration
- [ ] APR report export (Bilans stanja, Bilans uspeha)

Croatia:

- [ ] Legal review (Zakon o računovodstvu + GDPR)
- [ ] Croatian CoA seed data (RRiF)
- [ ] VAT at 25% / 13% / 5%
- [ ] FINA certificate for HR-FISK
- [ ] HR-FISK API integration (mandatory)
- [ ] FINA RGFI report export

Phase 3 — BiH Launch

- [ ] Legal review (FBiH + RS entity distinction)
- [ ] BiH CoA seed data (FBiH Pravilnik 2022)
- [ ] VAT at 17% (UIO)
- [ ] Monitor CPF specs (~2027)
- [ ] FBiH vs RS entity org settings

---

10. Risk Assessment

Risk	Likelihood	Impact	Mitigation

GDPR/ZZPL breach fine	Low (if compliant)	High (GDPR €20M / ZZPL RSD 2M)	Full implementation before first customer
SEF non-compliance (RS)	Medium	High (RSD 2M)	Phase 2 SEF integration
HR-FISK non-compliance (HR)	High (if not integrated)	Critical (EUR 500K)	Phase 2 mandatory
Financial data loss	Low	Critical	30-day Railway backups, immutable audit
Tax calculation error	Low	High	Configurable rates, NUMERIC precision, Zod
BiH CPF delay	Medium	Low	Phase 3 planned, not blocking RS/HR

Related Documents

- Security Architecture: security-architecture.md
- DPIA: data-protection-impact-assessment.md
- Breach Response Plan: data-breach-response-plan.md
- Bilko Compliance: ../../products/Bilko/docs/security/COMPLIANCE.md
- Serbia Regulatory: ../../products/Bilko/docs/regulatory/RS/README.md
- BiH Regulatory: ../../products/Bilko/docs/regulatory/BA/README.md
- Croatia Regulatory: ../../products/Bilko/docs/regulatory/HR/README.md

Approval

Role	Name	Date	Signature
Author	Compliance Architect	2026-02-23	
DPO			
Legal Counsel			
CEO			

Revision #8
Created 2026-02-24 14:52:39 UTC by John
Updated 2026-05-25 07:32:21 UTC by John