Compliance Framework

Compliance Framework Document

> **Project:** Bilko — Balkan Accounting SaaS **Version:** 1.0 **Date:** 2026-02-23 **Author:** DPO / Compliance Officer **Status:** Draft **Reviewers:** CTO, Legal Counsel (RS, BA, HR) **Classification:** Confidential

Document History

Version	Date	Author	Changes
0.1	2026-02-23	DPO	Initial three-country compliance mapping

---

1. Compliance Scope

Bilko is a cloud accounting SaaS operating in three jurisdictions. Each has distinct data protection, accounting, tax, and e-invoicing requirements.

```
graph TD
    subgraph RS["Serbia (Republika Srbija)"]
        RS_DP["ZZPL — Zakon o zaštiti podataka o ličnosti\nSl. glasnik RS 87/2018 (GDPR-aligned)"]
        RS_ACC["Zakon o računovodstvu\nSl. glasnik RS 73/2019"]
        RS_VAT["Zakon o PDV\n20% / 10% / 0%"]
        RS_SEF["SEF e-Invoice\nUBL 2.1 XML — B2B mandatory Jan 2023\nPenalty: 50K–2M RSD"]
        RS_APR["APR Filing\nJune 30 deadline"]
    end
```

```
    subgraph BA["Bosnia & Herzegovina"]
        BA_DP["ZZLP BiH — Zakon o zaštiti ličnih podataka\nSl. glasnik BiH 49/2006"]
        BA_FBiH["FBiH: Zakon o računovodstvu i reviziji FBiH\nSl. novine FBiH 83/2009 + Pravilnik 2022"]
        BA_RSBA["RS entitet: Zakon o računovodstvu i reviziji RS BiH\nSl. glasnik RS BiH 96/2005"]
        BA_VAT["Zakon o PDV BiH\n17% / 0% — UIO authority"]
        BA_CPF["CPF e-Invoice\nPending ~2027"]
    end

    subgraph HR["Croatia (Hrvatska)"]
        HR_DP["GDPR — directly applicable (EU member)\nUredba (EU) 2016/679"]
        HR_ACC["Zakon o računovodstvu\nNN 78/15, 116/18, 42/20, 47/20, 114/22"]
        HR_VAT["Zakon o porezu na dodanu vrijednost\n25% / 13% / 5% / 0%"]
        HR_FISK["HR-FISK (eRačun B2G/B2B)\nFINA certificate — mandatory Jan 2026\nPenalty: up to EUR 500K"]
        HR_FINA["FINA RGFI\nApril 30 deadline"]
    end
```

---

2. Data Protection Compliance

2.1 Applicable Laws

Jurisdiction	Law	Supervisory Authority	Penalty
Serbia	ZZPL (Sl. glasnik RS 87/2018)	Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti	Up to 2M RSD (legal entity)
Bosnia & Herzegovina	ZZLP BiH (Sl. glasnik BiH 49/2006)	Agencija za zaštitu ličnih podataka (AZLP)	Up to 10K BAM
Croatia	GDPR Uredba (EU) 2016/679	Agencija za zaštitu osobnih podataka (AZOP)	Up to €20M or 4% global turnover

2.2 Legal Basis for Processing

Data Category	Legal Basis	Jurisdiction
Account email, name	Contract performance (Art. 6(1)(b) GDPR / Art. 12(1)(b) ZZPL)	All

Data Category	Legal Basis	Jurisdiction
Tax IDs (PIB, JMBG, OIB, JIB)	Legal obligation — accounting/tax law	RS, BA, HR
IBAN, bank accounts	Contract performance	All
IP address, session logs	Legitimate interest — security	All
Financial transaction data	Legal obligation — accounting/tax law	All

2.3 Data Subject Rights Implementation

Right	GDPR Article	ZZPL Equivalent	Status
Access	Art. 15	Art. 26	Planned — `/api/gdpr/export` endpoint
Rectification	Art. 16	Art. 27	In-app edit functionality
Erasure ("Right to be forgotten")	Art. 17	Art. 28	Blocked by legal retention requirements
Portability	Art. 20	Art. 30	Planned — JSON/CSV export
Restriction	Art. 18	Art. 29	Planned — account suspension flow
Objection	Art. 21	Art. 31	Via support ticket

Note on Erasure: Financial data cannot be erased during mandatory retention periods (10 years RS, 10-11 years BA, 11 years HR). Account can be anonymized (name/email) but transaction records must be kept.

2.4 Cross-Border Data Transfers

- **Host:** Railway EU West (Amsterdam / Frankfurt) — within EEA
- **HR → Railway:** No transfer mechanism needed (EU to EU)
- **RS → Railway:** Serbia is on GDPR adequacy list (European Commission Decision 2023/1485)
- **BA → Railway:** No EU adequacy decision for BiH. Rely on Standard Contractual Clauses (SCC 2021/914) with Railway as processor.

2.5 DPA Requirements

Data Processing Agreements must be signed with:

- Railway (primary database host)
- Cloudflare (WAF, CDN — processes IP addresses)
- Sentry (error tracking — processes stack traces with potential PII)
- Any email service provider

3. Accounting & Tax Compliance

3.1 Serbia (RS)

Requirement	Law	Details	Bilko Implementation
Chart of Accounts	Pravilnik o kontnom okviru (Sl. glasnik RS 3/2020)	Standard Serbian CoA — 9 classes	RS-specific CoA template preloaded on org creation
VAT rates	Zakon o PDV (Sl. glasnik RS 84/2004 + amendments)	20% standard, 10% reduced, 0% exempt	VAT rate selector on invoice line items
Financial statements	Zakon o računovodstvu	Bilans stanja + Bilans uspeha (BS format)	Export to APR-compliant XML/PDF
Mandatory e-invoicing	Zakon o elektronskom fakturisanju (Sl. glasnik RS 44/2021)	B2B mandatory since Jan 1, 2023 (≥4.5M RSD)	SEF API integration (UBL 2.1 XML)
APR filing deadline	Zakon o računovodstvu Art. 33	June 30 (full-year entities), March 31 (other)	In-app reminder + export
Retention period	Zakon o računovodstvu Art. 26	10 years for financial statements and documentation	Delete-prevention lock on records >0 days old
Pausal regime	Zakon o paušalnom oporezivanju	<6M RSD annual income	Simplified invoice mode for pausal firms
PIO/health contributions	Zakon o doprinosima	Applied to salaries	Future: payroll module

SEF Integration:

- Portal: efaktura.mfin.gov.rs
- Format: UBL 2.1 XML (HR-CIUS compatible subset)
- Authentication: API key per organization
- Mandatory fields: seller PIB, buyer PIB, invoice number, date, amounts, VAT breakdown

3.2 Bosnia & Herzegovina (BA)

Requirement	Law	Details	Bilko Implementation
FBiH CoA	FBiH Pravilnik o računovodstvu (Sl. novine FBiH 89/2016 + 2022 revision)	FBiH-specific chart of accounts	FBiH CoA template
RS entity CoA	RS BiH Pravilnik	RS entity chart of accounts (differs from FBiH)	RS BiH CoA template

Requirement	Law	Details	Bilko Implementation
VAT rate	Zakon o PDV BiH (Sl. glasnik BiH 9/2005)	17% standard, 0% exempt — UIO authority	VAT 17% selector
VAT filing	UIO portal	Monthly/quarterly PDV prijava	Export to UIO-compatible format
Filing deadline	FBiH/RS entity laws	March 31 (most entities)	In-app reminder
FBiH retention	Zakon o računovodstvu i reviziji FBiH Art. 17	10 years	Delete-prevention lock
RS entity retention	Zakon o računovodstvu i reviziji RS BiH Art. 16	11 years	Delete-prevention lock
e-Invoice	CPF platform (pending)	Expected mandatory ~2027	Roadmap item
CIT rate	Zakon o porezu na dobit FBiH	10% flat	Future: tax calculation module

Entity detection: Bilko must determine if an organization is in FBiH, RS entity, or Brčko District to apply the correct CoA and retention rules. On org creation, user selects entity. Brčko follows BiH state-level law.

3.3 Croatia (HR)

Requirement	Law	Details	Bilko Implementation
CoA	Zakon o računovodstvu NN 78/15	Croatian standard CoA (HSFI / MSFI for large entities)	HR CoA template
Currency	Since Jan 2024: EUR only	HRK phased out. All amounts in EUR.	EUR default for HR orgs
VAT rates	Zakon o PDV (NN 73/13)	25% standard, 13% (food/hotels), 5% (books/medicines), 0%	VAT rate selector per line item
VAT filing	Porezna uprava	Monthly/quarterly PDV obrazac	Export for manual filing (Porezna uprava portal)
HR-FISK (eRačun)	Zakon o elektroničkom izdavanju računa u javnoj nabavi (NN 94/18) + amendments	Mandatory Jan 1, 2026 for B2B above threshold. FINA certificate required. UBL 2.1 XML HR-CIUS. Penalty up to EUR 500K	HR-FISK API integration — Roadmap P2
FINA RGFI filing	Zakon o računovodstvu Art. 30	April 30	In-app reminder + FINA export
Retention	Zakon o računovodstvu Art. 10 + Opći porezni zakon	11 years	Delete-prevention lock

Requirement	Law	Details	Bilko Implementation
Fiscalization 2.0	Pravilnik o fiskalizaciji	Cash register fiscalization (if cash payments)	Cash receipt module with Porezna uprava integration

HR-FISK Priority: Croatia's eRačun mandate (Jan 2026) with EUR 500K penalty makes this the highest-priority e-invoicing integration. FINA certificate must be obtained during onboarding for HR organizations.

---

4. Controls Register

Control ID	Description	Type	Applies To	Status
CC-01	AES-256-GCM encryption for L4 Restricted fields (PIB, JMBG, OIB, JIB, IBAN)	Technical	RS, BA, HR	Planned
CC-02	Organization-scoped WHERE on all Prisma queries	Technical	All	Planned
CC-03	RBAC with 4 roles (owner/admin/accountant/viewer)	Technical	All	Planned
CC-04	JWT RS256 with 15min expiry + refresh token rotation	Technical	All	Planned
CC-05	TLS 1.3 minimum via Cloudflare	Technical	All	Active
CC-06	LoggedAction audit trail (append-only, 10-11yr retention)	Technical	All	Planned
CC-07	DPA signed with Railway, Cloudflare, Sentry	Legal	All	Required pre-launch
CC-08	SEF integration for RS B2B e-invoicing	Technical	RS	P2 Roadmap
CC-09	HR-FISK integration + FINA certificate flow	Technical	HR	P2 Roadmap
CC-10	Data subject rights endpoints (/gdpr/export, /gdpr/delete)	Technical	All	Planned

Control ID	Description	Type	Applies To	Status
CC-11	72-hour breach notification procedure to Poverenik/AZLP/AZOP	Procedural	All	Required pre-launch
CC-12	Privacy Policy in Serbian, Bosnian, Croatian	Legal	RS, BA, HR	Required pre-launch
CC-13	Terms of Service with data processing consent	Legal	All	Required pre-launch
CC-14	VAT rate validation per jurisdiction	Technical	RS, BA, HR	Planned
CC-15	Retention lock preventing deletion of accounting records during mandatory retention period	Technical	All	Planned

5. Compliance Roadmap

```
gantt
    title Bilko Compliance Roadmap
    dateFormat  YYYY-MM

    section Phase 1 — MVP (pre-launch)
    GDPR/ZZPL core controls     : 2026-03, 2026-05
    DPAs signed                 : 2026-04, 2026-05
    Privacy Policy (3 languages) : 2026-04, 2026-05
    Terms of Service            : 2026-04, 2026-05
    DPIA completed              : 2026-04, 2026-05

    section Phase 2 — RS Launch
    SEF e-invoice integration   : 2026-06, 2026-08
    RS CoA + APR export         : 2026-06, 2026-07
    RS VAT reporting            : 2026-06, 2026-07

    section Phase 3 — BA Launch
    BA entity detection (FBiH vs RS) : 2026-09, 2026-10
    BA CoA templates            : 2026-09, 2026-10
```

```
    UIO VAT export               : 2026-09, 2026-10

    section Phase 4 — HR Launch
    HR-FISK + FINA cert flow     : 2026-10, 2026-12
    HR CoA + EUR amounts         : 2026-10, 2026-11
    Porezna uprava PDV export    : 2026-10, 2026-11
    FINA RGFI export             : 2026-10, 2026-11
```

Approval

Role	Name	Signature	Date
Author	DPO / Compliance Officer		2026-02-23
Reviewer (CTO)			
Reviewer (RS Legal)			
Reviewer (BA Legal)			
Reviewer (HR Legal)			
Approver	CEO		

Revision #3
Created 2026-02-24 22:50:53 UTC by John
Updated 2026-05-31 20:03:56 UTC by John