Bilko Privacy Notice — Section 8.1 Document Archive Sub-Processors

⚠ **STATUS**
MC: #100045 | **Date:** 2026-05-08
Draft Status: Pending final legal review and translations (per Lexicon S1-S4)
Corrections Applied: Org.nr 932 516 136 (corrected from hallucinated 933 534 262 + wrong DPO org.nr 932 953 736), Azure Sweden Central (corrected from Norway East)

Privacy Policy

> **Project:** Bilko — Balkan Accounting SaaS

> **Version:** 1.1

> **Last Updated:** 2026-03-02

> **Author:** ALAI Documentation Team

> **Status:** Final (Pending Legal Review)

> **Reviewers:** DPO, Legal Counsel (RS, BA, HR), CEO

> **Classification:** Public (upon legal sign-off)

Table of Contents

---

1. Introduction and Data Controller

Bilko is a cloud-based accounting and invoicing platform for small and medium businesses (SMBs) operating in Serbia, Bosnia & Herzegovina, and Croatia. Bilko is developed and operated by **Basic Consulting AS** (trading as ALAI), a company registered in Norway.

Data Controller:

Field	Details
---	---
Entity name	Basic Consulting AS (ALAI)
Registration	Pending — Norwegian company register number (to be confirmed upon legal entity formation)
Address	Pending — registered address to be confirmed upon legal entity formation

Email	privacy@bilko.io
Website	https://bilko.io

> ⚠ LEGAL REVIEW REQUIRED: Confirm whether Bilko must establish local legal entities in Serbia (Bilko d.o.o. RS), Bosnia & Herzegovina (Bilko d.o.o. Sarajevo), and Croatia (Bilko d.o.o. Zagreb) as co-controllers or separate controllers for purposes of local data protection law compliance. ZZPL Serbia and ZZLP BiH may require a locally registered representative.

Data Protection Officer (DPO):

FieldDetails ---------- DPO nameAlem Bašić DPO contactalem@alai.no Phone+47 40 47 42 51 CompanyALAI Holding AS (org.nr 932 516 136) RoleResponsible for data protection compliance across all three jurisdictions Appointed2026-03-02

2. Scope and Applicability

This Privacy Policy applies to:

- All users of the Bilko platform accessible at **app.bilko.io**
- All organizations registered on Bilko, including their authorized users (owners, admins, accountants, viewers)
- All data processed by Bilko in connection with providing cloud accounting services in Serbia, Bosnia & Herzegovina, and Croatia

This policy applies to **data subjects** in three categories:

- **Business owners and employees** who register and use Bilko directly
- **Clients and contacts** whose data is entered into Bilko by our users (e.g., customers listed on invoices)
- **Website visitors** to bilko.io

---

3. Legal Framework

Bilko processes personal data in compliance with the following data protection laws:

JurisdictionApplicable LawSupervisory Authority

---------- **Serbia**Zakon o zaštiti podataka o ličnosti (ZZPL), Sl. glasnik RS 87/2018 — aligned with GDPRPoverenik za informacije od javnog značaja i zaštitu podataka o ličnosti **Bosnia & Herzegovina**Zakon o zaštiti ličnih podataka (ZZLP BiH), Sl. glasnik BiH 49/2006Agencija za zaštitu ličnih podataka (AZLP) **Croatia**GDPR — Uredba (EU) 2016/679 (directly applicable as EU member state)Agencija za zaštitu osobnih podataka (AZOP)

Where GDPR principles are referenced in this policy, they apply directly to Croatian users and serve as the compliance standard for Serbian users (ZZPL is GDPR-aligned). For Bosnian users, equivalent provisions of ZZLP BiH apply.

---

4. Data We Collect

4.1 Account and Registration Data

When you register an organization on Bilko, we collect:

Data ElementPurposeClassification
---------- Email addressAccount authentication, notificationsL2 Internal Full nameUser identification within organizationL2 Internal Password (bcrypt-hashed)Authentication — never stored in plaintextL2 Internal Organization nameMulti-tenant account setupL2 Internal Country of operationJurisdiction-specific compliance rules (VAT rates, CoA)L2 Internal Base currencyFinancial calculationsL2 Internal

4.2 Financial and Tax Data

When you use Bilko to create invoices, track expenses, and manage accounting:

Data ElementJurisdictionClassificationEncryption
---------- PIB (Poreski identifikacioni broj — Serbia)RSL4-B RestrictedDisk-level AES-256 JMBG (Jedinstveni matični broj građana — Serbia/BiH)RS, BAL4-A RestrictedAES-256-GCM field-level OIB (Osobni identifikacijski broj — Croatia)HRL4-A RestrictedAES-256-GCM field-level JIB (Jedinstveni identifikacioni broj — BiH)BAL4-B RestrictedDisk-level AES-256 IBAN / Bank account numbersAllL4-B RestrictedDisk-level AES-256 + API masking Invoice amounts (subtotal, VAT, total)AllL3 ConfidentialAES-256 at rest Transaction records (debit/credit entries)AllL3 ConfidentialAES-256 at rest Expense recordsAllL3 ConfidentialAES-256 at rest Contact details (clients/vendors: name, email, phone, address)AllL2 InternalTLS 1.3 in transit

> **Note on JMBG processing:** The JMBG is a sensitive personal identifier unique to each Serbian and Bosnian citizen. Bilko only collects JMBG when a user explicitly confirms that an invoice is being issued to a natural person (not a legal entity). This is a voluntary user action gated by a UI confirmation checkbox.

4.3 Technical and Operational Data

Data ElementRetentionPurpose
---------- IP address30 daysSecurity monitoring, fraud detection Browser user-agent30 daysSecurity monitoring Session tokens (JWT, refresh tokens)15 minutes (access) / 7 days (refresh)Authentication Audit log entries (LoggedAction table)10–11 yearsLegal compliance, accounting law API request logs30 daysSecurity and debugging

4.4 Data Entered by Users About Third Parties

Bilko is an accounting tool. Our users enter data about their clients and vendors (third parties). This includes names, contact details, and tax identification numbers of those third parties. **Bilko acts as a data processor** for this third-party data — the organization using Bilko is the data controller for their clients' data and is responsible for ensuring they have an appropriate legal basis for entering that data into Bilko.

---

5. Legal Basis for Processing

Data CategoryLegal BasisGDPR ArticleZZPL ArticleZZLP BiH

Account email, full namePerformance of contractArt. 6(1)(b)Art. 12(1)(b)Art. 7(1)(b) Organization detailsPerformance of contractArt. 6(1)(b)Art. 12(1)(b)Art. 7(1)(b) Tax IDs (PIB, JIB)Legal obligation — accounting and tax lawArt. 6(1)(c)Art. 12(1)(c)Art. 7(1)(c) JMBG, OIBLegal obligation — accounting and tax law (only when legally required)Art. 6(1)(c)Art. 12(1)(c)Art. 7(1)(c) IBANPerformance of contract (for payment processing)Art. 6(1)(b)Art. 12(1)(b)Art. 7(1)(b) Invoice and transaction dataLegal obligation — accounting/tax retention requirementsArt. 6(1)(c)Art. 12(1)(c)Art. 7(1)(c) IP address, session logsLegitimate interest — platform securityArt. 6(1)(f)Art. 12(1)(f)Art. 7(1)(f) Audit trail (LoggedAction)Legal obligation — accounting law requires immutable audit recordsArt. 6(1)(c)Art. 12(1)(c)Art. 7(1)(c)

> ⚠ LEGAL REVIEW REQUIRED: Confirm the specific Serbian, Bosnian, and Croatian accounting and tax laws that constitute the "legal obligation" basis for each data category listed above. Reference: Zakon o računovodstvu RS (Sl. glasnik RS 73/2019), Zakon o PDV RS, Zakon o računovodstvu i reviziji FBiH, Zakon o porezu na dohodak FBiH, Zakon o računovodstvu HR (NN 78/15 et seq.).

---

6. How We Use Your Data

We use the data we collect exclusively to:

- **Provide the Bilko service** — create and manage invoices, expenses, transactions, financial reports
- **Ensure legal compliance** — submit e-invoices to SEF (Serbia) and HR-FISK (Croatia), maintain accounting records per mandatory retention periods
- **Secure the platform** — authenticate users, prevent unauthorized access, detect and investigate fraud and security incidents
- **Communicate with you** — send invoice notifications, payment reminders, service announcements, and support responses
- **Improve the service** — analyze usage patterns (in aggregated, anonymized form) to improve features

We do **not**:

- Sell your data to third parties
- Use your financial data for advertising or profiling
- Process your data for any purpose beyond providing the accounting service and meeting legal obligations

---

7. Data Retention Periods

Data retention is governed by accounting and tax laws in each jurisdiction. We are legally required to retain certain financial records even if you delete your account.

Data CategorySerbia (RS)Bosnia & Herzegovina (BA)Croatia (HR)Basis
--- Financial statements and accounting records10 yearsFBiH: 10 years; RS entity: 11 years11 yearsZakon o računovodstvu (RS/BA/HR) Invoice records10 years10–11 years11 yearsAccounting and VAT law Expense records10 years10–11 years11 yearsAccounting law Audit trail (LoggedAction)10 years10–11 years11 yearsAccounting law VAT/PDV records10 years10–11

years11 yearsTax law User account data (name, email)Account lifetime + 30 days after closureAccount lifetime + 30 daysAccount lifetime + 30 daysContract performance IP addresses and session logs30 days30 days30 daysLegitimate interest JWT refresh tokens7 days7 days7 daysContract performance

Important — Right to Erasure Limitation: Under accounting and tax law in all three jurisdictions, financial records (invoices, transactions, expense records) cannot be deleted during the mandatory retention period. If you close your Bilko account, your personal identifiers (name, email) can be anonymized in your user account record, but the underlying financial transaction data must be retained for the legally required period. See Section 10 for full details on data subject rights.

---

8. Data Sharing and Third-Party Processors

Bilko shares your data only with the following categories of third parties, all of whom are bound by Data Processing Agreements (DPAs):

ProcessorRoleData SharedLocationTransfer Mechanism

--- RailwayCloud infrastructure (PostgreSQL database, API hosting)All Bilko dataEU West (Amsterdam / Frankfurt)DPA — see Section 9 CloudflareCDN, WAF, DDoS protectionIP addresses, HTTP headersUSA (but data transits EU PoPs)DPA + Standard Contractual Clauses SentryError tracking and monitoringError traces, stack traces (may contain PII in error messages)USADPA + Standard Contractual Clauses Email service providerTransactional email (invoice delivery, notifications)Email addresses, invoice PDFsTBDDPA

> ⚠ LEGAL REVIEW REQUIRED: Select and confirm the transactional email service provider. Confirm DPA is in place with all processors above before launch. Cloudflare and Sentry are US-based — confirm SCC adequacy is sufficient for ZZPL and ZZLP BiH purposes, not just GDPR.

8.1 Document Archive Sub-Processors

When you enable the **document archival feature** in Bilko, the following additional sub-processors are used:

Sub-ProcessorPurposeData CategoriesLocationSafeguards

Cloudflare R2 (Cloudflare, Inc., USA)Temporary staging for archive pipelineContract PDFs, invoices, care plans, incident reports, onboarding documentsEU region (eu-west bucket)Standard Contractual Clauses (SCCs) **ALAI Azure VM Paperless-ngx** (ALAI Holding AS, org.nr 932 516 136, Norway)Long-term document archive at archive.alai.noSame categories as aboveEU/EEA (Microsoft Azure Sweden Central)ALAI DPA + Azure SCCs

How document archival works:

- **Upload:** When you mark a document for archival in Bilko (contracts, invoices, care plans, incident reports, onboarding documents), Bilko's backend writes the document to a Cloudflare R2 staging bucket in the EU region.

- **Transfer:** Every 5 minutes, a Cloud Run worker retrieves documents from R2 and uploads them to Paperless-ngx, a document management system hosted on ALAI's Azure VM (archive.alai.no) located in the Azure Sweden Central region (EU/EEA).

- **Retention:** Documents are retained in the archive according to the following schedule:

- **Financial documents** (invoices, contracts): **7 years** (Serbian Zakon o računovodstvu, BiH accounting law, Croatian Zakon o računovodstvu) - **Care-related documents** (care plans, incident reports): **25 years** (UK NHS retention standard; pending Balkan legal review for care organizations)

- **Deletion:** Documents are automatically deleted from Cloudflare R2 after successful upload to Paperless-ngx (typically within 5 minutes). Documents remain in Paperless-ngx for the retention period specified above.

Your rights regarding sub-processors (GDPR Art. 28(4)):

- You will receive **30 days' advance notice** by email before Bilko adds or replaces any sub-processor.
- You have the right to **object** to a new sub-processor within the notice period.
- If you object and Bilko cannot offer an alternative, you may terminate your subscription without penalty.
- Contact **dpa@alai.no** to exercise this right.
- This disclosure complies with GDPR Article 28(4), Serbian ZZPL Art. 31(4), and BiH ZZLP equivalent provisions.

Government Authorities:

When legally required, Bilko transmits e-invoice data to:

- **SEF portal** (efaktura.mfin.gov.rs) — Serbian Ministry of Finance — for RS users' B2B e-invoices
- **HR-FISK/FINA** — Croatian government e-invoicing authority — for HR users' B2B e-invoices (Phase 2)
- Tax and regulatory authorities in response to lawful requests

---

9. Cross-Border Data Transfers

Bilko hosts all data on Railway's EU West infrastructure (Amsterdam/Frankfurt). Data transfer mechanisms per jurisdiction:

FromToMechanism

--------- Croatia (HR)Railway EU WestNo transfer mechanism needed — EU to EU transfer Serbia (RS)Railway EU WestSerbia is on the European Commission's adequacy list (Decision 2023/1485) — no additional mechanism required Bosnia & Herzegovina (BA)Railway EU WestStandard Contractual Clauses (SCC 2021/914/EU) — BiH has no EU adequacy decision
For Cloudflare and Sentry (US-based processors): Standard Contractual Clauses (SCC) apply, combined with a Transfer Impact Assessment.

> ⚠ LEGAL REVIEW REQUIRED: Confirm that Serbia's adequacy decision (2023/1485) is still current and applies to the data categories Bilko processes. Prepare and sign SCCs with Railway for BiH user data before accepting Bosnian users. Conduct Transfer Impact Assessment for Cloudflare and Sentry.

---

10. Your Rights as a Data Subject

Depending on your jurisdiction, you have the following rights regarding your personal data:

10.1 Rights Table

RightGDPR (Croatia)ZZPL (Serbia)ZZLP BiHHow to Exercise

---------- **Right of access** — obtain a copy of your dataArt. 15Art. 26Art. 16Export via `/api/gdpr/export` (planned) or email privacy@bilko.io **Right to rectification** — correct inaccurate dataArt. 16Art. 27Art. 17Edit directly in Bilko settings, or email privacy@bilko.io **Right to erasure** — "right to be forgotten"Art. 17Art. 28Art. 18Email privacy@bilko.io — **subject to retention limitations below Right to data portability** — export in machine-readable formatArt. 20Art. 30N/A (not in ZZLP BiH)JSON/CSV export via Bilko (planned) **Right to restriction** — limit processingArt. 18Art. 29Art. 20Email privacy@bilko.io **Right to object** — object to processing based on legitimate interestArt. 21Art. 31Art. 21Email privacy@bilko.io **Right not to be subject to automated decisions**Art. 22Art. 38Art. 24Bilko does not make automated decisions with legal effect

10.2 Erasure Limitation (Financial Data)

The right to erasure does not apply to financial records that we are legally required to retain:

- In **Serbia**: Accounting records must be kept for **10 years** (Zakon o računovodstvu Art. 26)
- In **Bosnia & Herzegovina**: Records must be kept for **10–11 years** depending on entity
- In **Croatia**: Records must be kept for **11 years** (Zakon o računovodstvu Art. 10)

If you request erasure: your personal account information (name, email, password) can be deleted or anonymized, but underlying financial transaction records (invoices, expenses, journal entries) will be retained for the legally required period in anonymized or minimal form.

10.3 Response Times

We will respond to data subject rights requests within:

- **30 days** (standard) — may be extended by 2 additional months for complex requests with notification

10.4 Right to Complain

You have the right to lodge a complaint with your supervisory authority:

JurisdictionAuthorityWebsite ---------- SerbiaPoverenik za informacijepoverenik.rs Bosnia & HerzegovinaAZLPazlp.gov.ba CroatiaAZOPazop.hr

11. Security Measures

Bilko implements the following technical and organizational security measures to protect your data:

MeasureDescription

Encryption in transitTLS 1.3 (minimum TLS 1.2) for all connections via Cloudflare Encryption at restAES-256 disk-level encryption on all Railway infrastructure Field-level encryptionAES-256-GCM for JMBG (Serbia/BiH) and OIB (Croatia) — most sensitive personal identifiers IBAN maskingOnly last 4 digits shown in list views; full IBAN accessible only to authorized users Password securitybcrypt with cost factor 12; breached password check via HaveIBeenPwned API Authentication tokensJWT RS256, 15-minute access token lifetime, 7-day refresh with rotation Multi-tenancy isolationEvery database query is scoped to your organization — cross-tenant access is technically impossible by design Role-based access control4 roles (owner, admin, accountant, viewer) — users see only what their role permits Rate limiting5 failed authentication attempts per 15 minutes triggers lockout

Immutable audit logAll data modifications are recorded in an append-only audit trail Breach notification72-hour notification to supervisory authorities in the event of a personal data breach

---

12. Cookies and Tracking

Bilko uses minimal cookies necessary to provide the service:

CookiePurposeDuration ---------- `bilko_session` Stores encrypted session reference for authenticationSession `bilko_refresh` HTTP-only refresh token for session renewal7 days

> ⚠ LEGAL REVIEW REQUIRED: Confirm cookie consent requirements under Croatian GDPR (ePrivacy Directive applies in Croatia as EU member state). Serbia and BiH may have different requirements. Determine if a cookie consent banner is required.

We do not use third-party advertising cookies or tracking pixels.

---

13. Children's Privacy

Bilko is a business accounting platform intended for use by business owners and accounting professionals. We do not knowingly collect data from children under 16 years of age. If you believe a child has registered on Bilko, please contact privacy@bilko.io.

---

14. Changes to This Policy

We may update this Privacy Policy to reflect changes to our data practices or legal requirements. We will notify you of material changes by:

- Email to your registered account email address (at least 30 days before the change takes effect)
- Prominent notice on the Bilko platform

The date of the most recent revision is shown at the top of this document.

---

15. Contact and Data Protection Officer

For any privacy-related questions, requests, or complaints:

Privacy inquiries: privacy@bilko.io **Data Protection Officer:** Alem Bašić — alem@alai.no — +47 40 47 42 51 **DPO company:** ALAI Holding AS (org.nr 932 516 136) **Postal address:** Pending — to be confirmed upon company formation (see legal review note in Section 1)

> ⚠ LEGAL REVIEW REQUIRED: Confirm postal address for privacy contact in each jurisdiction. Consider whether a local representative must be designated in Serbia and BiH under their data protection laws.

---

16. Jurisdiction-Specific Notices

16.1 Serbia — Notice under ZZPL

This section applies specifically to users in the Republic of Serbia.

Bilko processes personal data in accordance with the **Zakon o zaštiti podataka o ličnosti** (Sl. glasnik RS 87/2018 — "ZZPL"). Your rights under ZZPL Articles 26–38 are described in Section 10 of this policy.

The supervisory authority for data protection in Serbia is the **Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti** (poverenik.rs).

Tax identification data (PIB) is processed pursuant to the **Zakon o poreskom postupku i poreskoj administraciji** and **Zakon o PDV**. Accounting records are retained pursuant to **Zakon o računovodstvu** (Sl. glasnik RS 73/2019) — minimum 10 years.

E-invoice data is submitted to the **SEF portal** (efaktura.mfin.gov.rs) pursuant to the **Zakon o elektronskom fakturisanju** (Sl. glasnik RS 44/2021). This transmission constitutes a legal obligation — no separate consent is required.

16.2 Bosnia & Herzegovina — Obavještenje prema ZZLP BiH

This section applies specifically to users in Bosnia & Herzegovina.

Bilko processes personal data in accordance with the **Zakon o zaštiti ličnih podataka** (Sl. glasnik BiH 49/2006 — "ZZLP BiH"). The supervisory authority is the **Agencija za zaštitu ličnih podataka (AZLP)** (azlp.gov.ba).

BiH has no EU adequacy decision. Data transferred to Railway (EU West) is protected by Standard Contractual Clauses (SCC 2021/914/EU).

Accounting records are retained pursuant to: FBiH — **Zakon o računovodstvu i reviziji FBiH** (minimum 10 years); RS entity — **Zakon o računovodstvu i reviziji RS BiH** (minimum 11 years). The correct retention period depends on the entity jurisdiction selected during organization registration.

> ⚠ LEGAL REVIEW REQUIRED: Confirm that the ZZLP BiH (2006 law) is still the governing framework or if amendments/successor legislation applies. Confirm AZLP registration requirements for Bilko as a data controller operating from outside BiH.

16.3 Croatia — Napomena prema GDPR-u

This section applies specifically to users in the Republic of Croatia.

As an EU member state, Croatia is subject to the **GDPR (Uredba (EU) 2016/679)** directly. The supervisory authority is the **Agencija za zaštitu osobnih podataka (AZOP)** (azop.hr).

Accounting records are retained pursuant to the **Zakon o računovodstvu** (NN 78/15, 116/18, 42/20, 47/20, 114/22) and **Opći porezni zakon** — minimum 11 years.

E-invoice data (when HR-FISK integration is active) is transmitted to **FINA** pursuant to the **Zakon o elektroničkom izdavanju računa u javnoj nabavi** and related legislation. This constitutes a legal obligation.

Approval

RoleNameSignatureDate ---------- AuthorALAI Documentation Team2026-02-25 DPO Review RS Legal Counsel BA Legal Counsel HR Legal Counsel CEO ApprovalAlem Bašić

Revision #4
Created 2026-05-08 19:55:46 UTC by John
Updated 2026-06-14 20:02:44 UTC by John