Security & Compliance

Security architecture, compliance framework, DPIA, data encryption policy, breach response, and security testing for Bilko.

Security Architecture

Bilko — Security Architecture

Status: PLANNED (backend not built yet, security measures documented for implementation)

This document defines the security architecture for Bilko, a financial SaaS handling sensitive accounting data.

Security Principles

1. **Defense in Depth** — Multiple layers of security (network, application, database)
2. **Least Privilege** — Users and services get minimum necessary permissions
3. **Zero Trust** — Verify every request, never assume trust
4. **Encryption Everywhere** — Data encrypted in transit and at rest
5. **Immutable Audit Trail** — All actions logged, tamper-proof

---

STRIDE Threat Model

Bilko handles sensitive financial data (tax IDs, IBAN, accounting records) across three jurisdictions. The STRIDE model identifies threats specific to each layer.

Spoofing — Identity Threats

Threat	Attack Vector	Bilko Risk	Mitigation
JWT token theft	XSS attack extracts access token from memory	HIGH — attacker gains full user session	CSP headers block inline scripts; access token not stored in localStorage
Session hijacking	Refresh token cookie stolen via network or MITM	HIGH — 7-day session takeover	httpOnly + Secure + SameSite=Strict cookie; TLS 1.3 only
Credential stuffing	Automated login with leaked credentials	HIGH — financial platform targeted	Rate limiting (5 req/15min); bcrypt 12 rounds; HIBP breach check

Threat	Attack Vector	Bilko Risk	Mitigation
JWT algorithm confusion	Attacker sends `alg: none` or switches HS256/RS256	MEDIUM	`jsonwebtoken` always specifies algorithm explicitly; RS256 enforced
Account enumeration	Timing attack on login endpoint reveals valid emails	MEDIUM	Constant-time response regardless of email existence

Tampering — Data Integrity Threats

Threat	Attack Vector	Bilko Risk	Mitigation
Invoice amount modification	MITM attack modifies invoice amounts in transit	HIGH — financial fraud	TLS 1.3 for all connections; HSTS with preload
Transaction record alteration	Unauthorized user modifies financial records	CRITICAL — accounting integrity	LoggedAction audit trail (append-only); Prisma soft delete only
JWT payload manipulation	Attacker decodes JWT, changes `role: viewer` to `role: owner`	HIGH — privilege escalation	RS256 signature verification; any modification invalidates signature
Database record tampering	Direct DB access bypasses application	HIGH — data integrity loss	Railway access restricted to CTO only; no public DB port
File upload replacement	Upload modified invoice PDF with different amounts	MEDIUM	File stored by hash; original uploaded by authorized user; audit trail

Repudiation — Non-Traceability Threats

Threat	Attack Vector	Bilko Risk	Mitigation
Audit log bypass	Attacker finds code path that skips LoggedAction	HIGH — undetected fraud	Prisma middleware applies audit to ALL model mutations; test coverage
LoggedAction deletion	Admin or attacker deletes audit records	CRITICAL — compliance violation	LoggedAction has no DELETE permission in RBAC; DB-level row security planned
Timestamp manipulation	System clock skewed to invalidate audit timestamps	LOW	Railway NTP; JWT `iat` verified server-side
User denies action	"I never deleted that invoice"	MEDIUM	Audit log captures: userId, IP, exact timestamp, old values, new values

Information Disclosure — Data Leakage Threats

Threat	Attack Vector	Bilko Risk	Mitigation
Cross-tenant data leak	Missing `organizationId` WHERE clause on Prisma query	CRITICAL — GDPR breach	Org-scoping middleware on all routes; lint rule + automated isolation tests
Financial data in API errors	Stack trace contains query with financial amounts	HIGH	Production error handler returns only generic message + error ID
Tax ID (JMBG/OIB) exposure	DB breach exposes plaintext personal citizen IDs	CRITICAL — identity theft, irrevocable	AES-256-GCM field-level encryption (Tier 1) via prisma-field-encryption (See ADR-014)
Tax ID (PIB/JIB) exposure	DB breach exposes business tax IDs	LOW — publicly available on APR/UIO portals	Disk-level encryption (Railway AES-256) + org-scoping + RBAC (Tier 2, See ADR-014)
IBAN exposure	DB breach or API response over-returning	MEDIUM — routinely shared for payment	Disk-level encryption + IBAN masked in list responses (last 4 digits only) (See ADR-014)
JWT contains PII	Access token readable by any party	MEDIUM	JWT contains only user ID, org ID, role — no email, name, or financial data
Log file leakage	Application logs contain email addresses or amounts	MEDIUM	Logging policy: never log request body for financial endpoints

Denial of Service — Availability Threats

Threat	Attack Vector	Bilko Risk	Mitigation
Authentication flooding	Brute force login with millions of requests	HIGH	Rate limiting: 5 requests/15min on auth endpoints; Cloudflare DDoS protection
Report generation abuse	Repeated complex report requests exhaust DB	MEDIUM	Rate limiting: 10 requests/15min on `/api/v1/reports/*`; caching layer planned
File upload flooding	Upload large files repeatedly	MEDIUM	10MB limit; multer request counting; Cloudflare rate limiting at edge
Database connection exhaustion	Many concurrent requests exceed pool size	MEDIUM	Prisma connection pool limits; Railway auto-scaling

Threat	Attack Vector	Bilko Risk	Mitigation
Webhook replay flooding	Repeat webhook calls to SEF/FINA integration	LOW	Idempotency keys on e-invoice submissions; webhook signature verification

Elevation of Privilege — Access Control Threats

Threat	Attack Vector	Bilko Risk	Mitigation
RBAC bypass via role tampering	Modify JWT role claim to gain admin access	CRITICAL	RS256 signature; role read from verified JWT payload only
Cross-tenant elevation	Org-1 user accesses Org-2 resources by guessing UUID	HIGH — multi-tenant SaaS	UUID v4 unpredictable; org-scoped WHERE mandatory; 404 (not 403) on cross-org requests
Horizontal privilege escalation	Accountant accesses another user's profile in same org	MEDIUM	Per-user data scoped by `userId`; endpoints check `req.user.id === resource.userId`
API endpoint enumeration	Attacker discovers undocumented admin endpoints	LOW	No hidden admin endpoints; all endpoints in API spec; Cloudflare WAF
Dependency hijacking	Malicious package injected via supply chain	MEDIUM	`package-lock.json` committed; Dependabot; npm audit in CI

Authentication

Strategy: JWT (JSON Web Tokens)

Why JWT?

- Stateless (scales horizontally)
- Works with mobile PWA
- Industry standard

Token Types

Access Token

- **Lifetime:** 15 minutes
- **Storage:** `Authorization: Bearer <token>` header
- **Contains:** User ID, organization ID, role
- **Refresh:** Automatic via refresh token

Refresh Token

- **Lifetime:** 7 days
- **Storage:** httpOnly cookie (not accessible to JavaScript)
- **Purpose:** Obtain new access token
- **Rotation:** New refresh token issued on each refresh
- **Revocation:** Stored in database, can be invalidated

JWT Payload Example

```
{
  "sub": "user-uuid",
  "org": "org-uuid",
  "role": "admin",
  "iat": 1640000000,
  "exp": 1640000900,
  "jti": "unique-token-id"
}
```

> `jti` (JWT ID) — unique token identifier used to prevent replay attacks and enable server-side token invalidation.

Token Flow

```
1. User logs in → POST /api/v1/auth/login
   ← Access token (header) + Refresh token (httpOnly cookie)

2. User makes request → GET /api/v1/invoices (Authorization: Bearer <access>)
   ← Protected resource

3. Access token expires (15 min) → POST /api/v1/auth/refresh (httpOnly cookie)
   ← New access token + New refresh token

4. User logs out → POST /api/v1/auth/logout
```

```
   → Delete refresh token from DB
   ← 204 No Content
```

Implementation (Backend)

```
import jwt from 'jsonwebtoken';
import bcrypt from 'bcrypt';

// Generate access token
const accessToken = jwt.sign(
  { sub: user.id, org: user.organizationId, role: user.role },
  process.env.JWT_SECRET!,
  { expiresIn: '15m' }
);

// Generate refresh token
const refreshToken = jwt.sign(
  { sub: user.id },
  process.env.JWT_REFRESH_SECRET!,
  { expiresIn: '7d' }
);

// Store refresh token in DB (for revocation)
await prisma.refreshToken.create({
  data: {
    token: refreshToken,
    userId: user.id,
    expiresAt: new Date(Date.now() + 7 * 24 * 60 * 60 * 1000),
  },
});
```

Token Invalidation Events

Refresh tokens must be revoked server-side on any of these events:

- User logout
- Password change
- Role change by admin
- Account suspension
- Suspicious login from unknown IP/country

Password Security

Hashing: bcrypt

Algorithm: bcrypt with 12 salt rounds

Why bcrypt?

- Designed for passwords (slow by design, resists brute force)
- Auto-salted (each password has unique salt)
- Adaptive (can increase rounds as hardware improves)

Password Requirements

- **Minimum length:** 8 characters
- **Complexity:** At least one uppercase, one lowercase, one number
- **No common passwords:** Check against list of 10K most common passwords
- **No reuse:** Previous 5 passwords stored (hashed) and blocked

Implementation

```
import bcrypt from 'bcrypt';

// Hash password (registration)
const passwordHash = await bcrypt.hash(password, 12);

// Verify password (login)
const isValid = await bcrypt.compare(password, user.passwordHash);
```

Two-Factor Authentication (2FA)

Strategy: TOTP (Time-based One-Time Password)

Compatible with:

- Google Authenticator
- Authy
- 1Password
- Microsoft Authenticator

Setup Flow

```
1. User enables 2FA → POST /api/v1/auth/2fa/setup
   ← QR code + secret (base32)

2. User scans QR code in authenticator app
   → Generates 6-digit code

3. User verifies code → POST /api/v1/auth/2fa/verify { code }
   ← 200 OK (2FA enabled)
```

Login Flow with 2FA

```
1. User logs in → POST /api/v1/auth/login { email, password }
   ← 200 OK + { requires2FA: true, tempToken }

2. User enters code → POST /api/v1/auth/2fa/login { tempToken, code }
   ← Access token + Refresh token
```

Backup Codes

Generate 10 single-use backup codes during 2FA setup:

- Stored hashed (bcrypt)
- Used when authenticator unavailable
- Marked as used after redemption

Authorization (RBAC)

Roles

Role	Permissions

owner	Full access (edit org settings, invite users, delete data)
admin	Manage invoices, expenses, contacts, reports (no org settings)
accountant	Read invoices/expenses, create reports (no edit)
viewer	Read-only access (dashboard, reports)

Permission Matrix

Action	owner	admin	accountant	viewer
Create invoice	□	□	□	□
Edit invoice	□	□	□	□
Delete invoice	□	□	□	□
View invoice	□	□	□	□
Approve expense	□	□	□	□
Generate report	□	□	□	□
Invite user	□	□	□	□
Edit org settings	□	□	□	□

Implementation (Middleware)

```
import { Request, Response, NextFunction } from 'express';

function requireRole(roles: string[]) {
  return (req: Request, res: Response, next: NextFunction) => {
    if (!roles.includes(req.user.role)) {
      return res.status(403).json({ error: 'Forbidden' });
    }
    next();
  };
}

// Usage
app.post('/api/v1/invoices', requireRole(['owner', 'admin']), createInvoice);
```

Data Classification

Level	Label	Examples	Controls
L4-A	Restricted (Personal)	JMBG, OIB	AES-256-GCM field-level encryption (prisma-field-encryption) + HMAC-SHA256 hash columns + access log (See ADR-014)
L4-B	Restricted (Business/Financial)	PIB, JIB, IBAN	Disk-level encryption (Railway AES-256) + TLS 1.3 + org-scoping + RBAC + API masking for IBAN (last 4 digits) (See ADR-014)
L3	Confidential	Financial amounts, bank statements, invoices	Org-scoped access, TLS, PostgreSQL AES-256 at rest
L2	Internal	Email, name, address, phone	TLS, authenticated access only
L1	Public	Organization name, public invoice reference	No special controls

L4 Restricted fields use a hybrid encryption approach per ADR-014: personal identifiers (JMBG, OIB) receive AES-256-GCM field-level encryption before persistence because they are irrevocable and high-impact on breach. Business tax IDs (PIB, JIB) and IBAN rely on disk-level encryption plus application-layer controls — field-level encryption for publicly available identifiers would be disproportionate to the risk per GDPR Article 32.

Encryption

In Transit: TLS 1.3

All traffic encrypted via HTTPS:

- Frontend (Vercel): Automatic HTTPS
- Backend (Railway): Automatic HTTPS
- Certificate: Let's Encrypt (auto-renewed)

TLS Configuration:

- Minimum version: TLS 1.3
- Cipher suites: Modern only (no legacy ciphers)
- HSTS enabled (Strict-Transport-Security header)

At Rest: Database Encryption

PostgreSQL (Railway):

- Disk encryption: AES-256 (Railway default)
- Backup encryption: AES-256
- Column-level encryption: **Hybrid approach per ADR-014** — JMBG and OIB fields use AES-256-GCM field-level encryption via `prisma-field-encryption` (Tier 1). PIB, JIB, and IBAN rely on disk-level encryption + application controls (Tier 2). Disk-level encryption alone is insufficient for personal identifiers (JMBG/OIB) due to their irrevocability and high breach impact. (See ADR-014)

Cloudflare R2 (Files):

- Server-side encryption: AES-256 (default)
- No client-side encryption needed (files are receipts/invoices, not PII)

Secrets Management

NEVER commit secrets to git:

- `.env` files in `.gitignore`
- Use platform-provided secrets (Vercel, Railway)
- Rotate JWT secrets quarterly
- Rotate API keys annually

OWASP Top 10 Mitigations

1. Injection (SQL Injection)

Mitigation: Prisma ORM parameterized queries

```
// SAFE — Prisma auto-escapes
await prisma.invoice.findMany({
  where: { customerId: req.params.id }
});

// UNSAFE — Never use raw SQL for user input
await prisma.$queryRaw`SELECT * FROM invoices WHERE customer_id = ${req.params.id}`;
```

---

2. Broken Authentication

Mitigations:

- bcrypt password hashing (12 rounds)
- JWT with short expiry (15 min)
- Refresh token rotation
- 2FA (TOTP)
- Rate limiting on auth endpoints (5 req/min)

---

3. Sensitive Data Exposure

Mitigations:

- TLS 1.3 in transit
- AES-256 at rest
- No PII in JWTs (only user ID)
- No passwords in logs
- No sensitive data in URLs (use POST body)

---

4. XML External Entities (XXE)

Not applicable — Bilko does not parse XML.

---

5. Broken Access Control

Mitigations:

- RBAC enforced on every endpoint
- Organization-scoped queries (middleware)
- No direct object reference (use UUIDs, not auto-increment IDs)

```
// Organization scoping middleware
app.use('/api/v1/*', (req, res, next) => {
  req.prismaWhere = { organizationId: req.user.organizationId };
  next();
});

// Apply to queries
```

```
await prisma.invoice.findMany({ where: req.prismaWhere });
```

6. Security Misconfiguration

Mitigations:

- Helmet.js security headers
- CORS whitelist (no `*` in production)
- Error messages sanitized (no stack traces in production)
- Disable `X-Powered-By` header

Full Security Headers Configuration

All security headers applied via Helmet.js on the Express API. The Next.js frontend applies equivalent headers via `next.config.js`.

```
import helmet from 'helmet';

// Express API — full security headers
app.use(helmet({
  // Content-Security-Policy — prevent XSS
  contentSecurityPolicy: {
    directives: {
      defaultSrc: ["'self'"],
      scriptSrc: ["'self'"],           // No unsafe-inline needed on API
      styleSrc: ["'self'"],
      imgSrc: ["'self'", "data:"],
      connectSrc: ["'self'"],
      frameSrc: ["'none'"],            // No iframes from this API
      objectSrc: ["'none'"],
      upgradeInsecureRequests: [],
    },
    useDefaults: false,
  },
  // Strict-Transport-Security — force HTTPS for 1 year, include subdomains
  hsts: {
    maxAge: 31536000,                  // 1 year in seconds
    includeSubDomains: true,
    preload: true,                     // Eligible for browser HSTS preload list
  },
```

```
  // X-Frame-Options — prevent clickjacking
  frameguard: {
    action: 'deny',                    // DENY: no framing at all
  },
  // X-Content-Type-Options — prevent MIME sniffing
  noSniff: true,
  // X-XSS-Protection — legacy header for older browsers
  xssFilter: true,
  // Referrer-Policy — don't leak URL in Referer header
  referrerPolicy: {
    policy: 'strict-origin-when-cross-origin',
  },
  // Permissions-Policy — disable browser features not needed by Bilko
  permittedCrossDomainPolicies: { permittedPolicies: 'none' },
  // X-DNS-Prefetch-Control
  dnsPrefetchControl: { allow: false },
  // X-Powered-By removed by default in Helmet
  hidePoweredBy: true,
}));

// Permissions-Policy header (not yet in Helmet — set manually)
app.use((req, res, next) => {
  res.setHeader(
    'Permissions-Policy',
    'camera=(), microphone=(), geolocation=(), payment=(), usb=()'
  );
  next();
});

// CORS — whitelist only known origins
app.use(cors({
  origin: (origin, callback) => {
    const allowed = [
      'https://bilko.io',
      'https://www.bilko.io',
      'https://app.bilko.io',
      'https://staging.bilko.io',
      'https://bilko.rs',     // Serbia redirect domain
    ];
    if (!origin || allowed.includes(origin)) {
```

```
      callback(null, true);
    } else {
      callback(new Error(`CORS: origin ${origin} not allowed`));
    }
  },
  credentials: true,                    // Required for httpOnly cookie (refresh token)
  methods: ['GET', 'POST', 'PUT', 'PATCH', 'DELETE', 'OPTIONS'],
  allowedHeaders: ['Content-Type', 'Authorization'],
}));
```

Next.js Frontend Security Headers (`next.config.js`)

```
// next.config.js
const securityHeaders = [
  {
    key: 'Content-Security-Policy',
    value: [
      "default-src 'self'",
      "script-src 'self' 'unsafe-inline' 'unsafe-eval'",  // Next.js requires these
      "style-src 'self' 'unsafe-inline'",                  // Tailwind requires unsafe-inline
      "img-src 'self' data: https:",
      "connect-src 'self' https://api.bilko.io wss://api.bilko.io",
      "font-src 'self' https://fonts.gstatic.com",
      "frame-ancestors 'none'",
      "upgrade-insecure-requests",
    ].join('; '),
  },
  { key: 'Strict-Transport-Security', value: 'max-age=31536000; includeSubDomains; preload' },
  { key: 'X-Frame-Options', value: 'DENY' },
  { key: 'X-Content-Type-Options', value: 'nosniff' },
  { key: 'Referrer-Policy', value: 'strict-origin-when-cross-origin' },
  { key: 'Permissions-Policy', value: 'camera=(), microphone=(), geolocation=(), payment=()'
},
  { key: 'X-DNS-Prefetch-Control', value: 'off' },
];

module.exports = {
  headers: async () => [
    { source: '/:path*', headers: securityHeaders },
  ],
```

```
};
```

Headers Verification

Use securityheaders.com to verify. Target grade: **A+**.

Header	Expected Value	Purpose
`Content-Security-Policy`	Restrictive directives	Prevent XSS
`Strict-Transport-Security`	`max-age=31536000; includeSubDomains; preload`	Force HTTPS
`X-Frame-Options`	`DENY`	Prevent clickjacking
`X-Content-Type-Options`	`nosniff`	Prevent MIME sniffing
`Referrer-Policy`	`strict-origin-when-cross-origin`	Limit referrer leakage
`Permissions-Policy`	Disable camera/mic/geo/payment	Minimize attack surface

---

7. Cross-Site Scripting (XSS)

Mitigations:

- React auto-escapes output (default safe)
- CSP headers (Content-Security-Policy)
- Sanitize user input (Zod validation)
- No `dangerouslySetInnerHTML` without sanitization

```
// SAFE — React escapes by default
<p>{invoice.description}</p>

// UNSAFE — Only use with sanitized HTML
<div dangerouslySetInnerHTML={{ __html: sanitizedHTML }} />
```

---

8. Insecure Deserialization

Not applicable — Bilko does not deserialize untrusted data.

---

9. Using Components with Known Vulnerabilities

Mitigations:

- Dependabot alerts enabled (GitHub)
- Weekly `npm audit` checks
- Automated security updates (Dependabot PRs)
- Lock file committed (`package-lock.json`)

---

10. Insufficient Logging & Monitoring

Mitigations:

- Audit trail (LoggedAction table)
- Error tracking (Sentry recommended)
- Access logs (Railway built-in)
- Failed login attempts logged
- Anomaly detection (future: alert on 10+ failed logins)

Rate Limiting

Prevent brute force and abuse:

Endpoint	Limit	Window	Rationale
`/api/v1/auth/login`	5 requests	15 minutes	Prevent credential stuffing
`/api/v1/auth/register`	3 requests	60 minutes	Prevent bulk account creation
`/api/v1/auth/refresh`	10 requests	15 minutes	Prevent refresh token flood
`/api/v1/auth/2fa/login`	5 requests	15 minutes	Prevent TOTP brute force
`/api/v1/auth/forgot-password`	3 requests	60 minutes	Prevent email enumeration via flood
`/api/v1/*` (general)	100 requests	15 minutes	General API protection
`/api/v1/reports/*`	10 requests	15 minutes	Prevent expensive query abuse
`/api/v1/*/export`	5 requests	60 minutes	Prevent bulk data export

Implementation

```
import rateLimit from 'express-rate-limit';
import RedisStore from 'rate-limit-redis';
```

```
// Auth limiter — strict
const authLimiter = rateLimit({
  windowMs: 15 * 60 * 1000,            // 15 minutes
  max: 5,
  standardHeaders: true,
  legacyHeaders: false,
  message: { error: 'Too many attempts. Try again in 15 minutes.' },
  // Use IP + email combination as key to prevent distributed attacks
  keyGenerator: (req) => `${req.ip}:${req.body?.email ?? 'unknown'}`,
});

// General API limiter
const generalLimiter = rateLimit({
  windowMs: 15 * 60 * 1000,
  max: 100,
  standardHeaders: true,
  legacyHeaders: false,
  skip: (req) => isWebhookRequest(req), // Webhooks bypass general limiter
});

app.post('/api/v1/auth/login', authLimiter, loginHandler);
app.use('/api/v1/', generalLimiter);
```

IP Whitelisting for Webhooks

Webhooks from SEF (Serbian e-invoice portal) and FINA (Croatian HR-FISK) must bypass general rate limiting but are restricted to known IP ranges:

```
// Known webhook source IP ranges
const SEF_WEBHOOK_IPS = [
  '185.54.144.0/24',   // efaktura.mfin.gov.rs — verify with SEF portal docs
];

const FINA_WEBHOOK_IPS = [
  '195.29.61.0/24',    // FINA PKI infrastructure — verify with FINA
];

function isWebhookRequest(req: Request): boolean {
  const clientIp = req.ip ?? req.socket.remoteAddress;
  return [...SEF_WEBHOOK_IPS, ...FINA_WEBHOOK_IPS].some(
```

```
    (range) => ipRangeContains(range, clientIp)
  );
}

// Webhook endpoint — IP-restricted, no general rate limit
app.post('/api/v1/webhooks/sef',
  requireWebhookIp(SEF_WEBHOOK_IPS),
  verifyWebhookSignature,
  handleSefWebhook
);

app.post('/api/v1/webhooks/fina',
  requireWebhookIp(FINA_WEBHOOK_IPS),
  verifyWebhookSignature,
  handleFinaWebhook
);

function requireWebhookIp(allowedRanges: string[]) {
  return (req: Request, res: Response, next: NextFunction) => {
    const clientIp = req.ip ?? req.socket.remoteAddress;
    const allowed = allowedRanges.some((range) => ipRangeContains(range, clientIp));
    if (!allowed) {
      return res.status(403).json({ error: 'Webhook source IP not allowed' });
    }
    next();
  };
}
```

Note: Confirm exact SEF and FINA IP ranges from their integration documentation before deployment. Update `SEF_WEBHOOK_IPS` and `FINA_WEBHOOK_IPS` accordingly.

Input Validation

All inputs validated with **Zod** schemas:

Example: Invoice Validation

```
import { z } from 'zod';

const createInvoiceSchema = z.object({
  customerId: z.string().uuid(),
  invoiceDate: z.string().regex(/^\d{4}-\d{2}-\d{2}$/),
  dueDate: z.string().regex(/^\d{4}-\d{2}-\d{2}$/),
  currencyCode: z.enum(['EUR', 'RSD', 'BAM', 'HRK']),
  items: z.array(z.object({
    description: z.string().min(1).max(500),
    quantity: z.number().positive(),
    unitPrice: z.number().nonnegative(),
    taxRate: z.number().min(0).max(100),
  })),
});

// Middleware
function validate(schema: z.ZodSchema) {
  return (req, res, next) => {
    try {
      req.body = schema.parse(req.body);
      next();
    } catch (error) {
      res.status(400).json({ error: error.errors });
    }
  };
}

// Usage
app.post('/api/v1/invoices', validate(createInvoiceSchema), createInvoice);
```

File Upload Security

Allowed File Types

- **Receipts:** JPG, PNG, PDF
- **Max size:** 10MB per file

Validation

```
import multer from 'multer';
import path from 'path';

const upload = multer({
  limits: { fileSize: 10 * 1024 * 1024 }, // 10MB
  fileFilter: (req, file, cb) => {
    const allowedTypes = ['.jpg', '.jpeg', '.png', '.pdf'];
    const ext = path.extname(file.originalname).toLowerCase();
    if (allowedTypes.includes(ext)) {
      cb(null, true);
    } else {
      cb(new Error('Invalid file type'));
    }
  },
});
```

Virus Scanning (Planned)

Phase 2: Integrate ClamAV for virus scanning before upload to R2.

Audit Trail

LoggedAction Table (Immutable)

All mutations logged:

- Table name
- Action (INSERT, UPDATE, DELETE)
- User ID
- Timestamp
- Old values (UPDATE/DELETE)
- New values (INSERT/UPDATE)
- Client IP
- SQL query

Example Audit Log Entry

```
{
  "eventId": 12345,
  "tableName": "invoices",
  "action": "UPDATE",
  "userId": "user-uuid",
  "actionTimestamp": "2026-02-20T10:30:00Z",
  "rowData": { "id": "invoice-uuid", "status": "draft" },
  "changedFields": { "status": { "old": "draft", "new": "sent" } },
  "clientIp": "192.168.1.10"
}
```

Audit Queries

```
// Get user activity
await prisma.loggedAction.findMany({
  where: { userId: 'user-uuid' },
  orderBy: { actionTimestamp: 'desc' },
  take: 100,
});

// Get invoice history
await prisma.loggedAction.findMany({
  where: {
    tableName: 'invoices',
    rowData: { path: ['id'], equals: 'invoice-uuid' },
  },
});
```

Data Retention & Deletion

User Data Deletion (GDPR Right to Erasure)

Process:

1. User requests deletion → POST /api/v1/account/delete
2. Soft delete user record (mark `deletedAt`)
3. Anonymize LoggedAction entries (replace user ID with "deleted-user")
4. Delete PII (email, name)

5. **Keep financial records** (required by law, minimum 5 years)

Soft Delete Implementation:

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

Security Testing

Static Analysis

- **ESLint:** Security rules enabled (no-eval, no-unsafe-regex)
- **TypeScript:** Strict mode (catches type errors)

Dependency Scanning

- **npm audit:** Weekly checks
- **Dependabot:** Automatic PRs for vulnerabilities

Penetration Testing Plan

Frequency: Annual + after significant architecture changes **Provider:** External certified firm (OSCP or CREST certified) **Environment:** Staging only (`staging.bilko.io`) — **never production without explicit CEO approval**

Scope

Area	Priority	Test Approach
Authentication & session management	P0 — Critical	JWT tampering, refresh token theft, brute force, 2FA bypass
Multi-tenant data isolation	P0 — Critical	Cross-org data access, IDOR on UUIDs, query manipulation

Area	Priority	Test Approach
RBAC & privilege escalation	P1 — High	Role tampering, horizontal escalation, missing authorization
API security	P1 — High	All endpoints for injection, auth bypass, mass assignment
Financial data protection	P1 — High	Encrypted field bypass, IBAN/tax ID extraction
File upload security	P2 — Medium	Malicious file upload, path traversal, SSRF
Third-party integrations	P2 — Medium	SEF / FINA webhook manipulation, replay attacks
Business logic	P2 — Medium	Invoice amount manipulation, VAT calculation errors, status bypass

Pre-Engagement Checklist

- ☐ Statement of Work (SoW) signed with pentest firm
- ☐ Staging environment set up with production-equivalent configuration
- ☐ Test data (fake organizations, fake invoices) loaded — **no real customer data**
- ☐ Bilko DBA grants read-only DB access to pentest firm for review (not write)
- ☐ Confirm staging SEF/FINA integrations are in test mode
- ☐ Legal: pentest authorization letter from CEO on file

Acceptance Criteria

- **Zero Critical or High findings** unmitigated before production launch
- **Medium findings**: each assessed, documented, and either fixed or accepted with justification
- **Remediation SLAs:**
  - CRITICAL: 48 hours
  - HIGH: 7 days
  - MEDIUM: 30 days
  - LOW: Next sprint boundary

Pentest Report Requirements

The pentest report must include:

1. Executive summary (risk level, critical findings)
2. Technical findings: CVSS score, proof of concept, affected endpoints
3. Business impact statement for each finding
4. Remediation recommendations
5. Re-test results (confirm fixes for Critical and High)

Incident Response Plan

Detection

- Monitor error rates (Sentry)
- Monitor failed login attempts (>10 in 1 hour = alert)
- Railway metrics (CPU spike, memory leak)

Response

1. **Identify:** What is the breach? (data leak, DDoS, unauthorized access)
2. **Contain:** Block attacker IP, revoke compromised tokens
3. **Eradicate:** Fix vulnerability, patch code
4. **Recover:** Restore from backup if needed
5. **Document:** Write post-mortem, update security docs

Notification

- **Internal:** Slack alert to #security channel
- **External:** Email users if PII compromised (GDPR 72h requirement)

Security Checklist (Pre-Launch)

- ☐ JWT secrets generated (32+ chars)
- ☐ HTTPS enforced (no HTTP allowed)
- ☐ CORS whitelist configured (no `*`)
- ☐ Rate limiting enabled (auth endpoints)
- ☐ Helmet.js security headers configured
- ☐ bcrypt password hashing (12 rounds)
- ☐ Prisma queries parameterized (no raw SQL)
- ☐ Input validation (Zod schemas)
- ☐ File upload restrictions (type, size)
- ☐ Audit trail enabled (LoggedAction)
- ☐ Error messages sanitized (no stack traces)

- [ ] Dependabot alerts enabled
- [ ] Backup strategy tested
- [ ] Incident response plan documented
- [ ] Security review completed

Related Documents

- Compliance: COMPLIANCE.md
- Deployment: ../infrastructure/DEPLOYMENT.md
- Testing: ../testing/TESTING-GUIDE.md

Last Updated: 2026-02-20 **Status:** PLANNED — Backend not built yet, security measures to be implemented **Compliance:** OWASP Top 10, GDPR Article 32 (Security of Processing)

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
Tax IDs (PIB, JMBG, OIB, JIB)	Legal obligation — accounting/tax law	RS, BA, HR

Data Category	Legal Basis	Jurisdiction
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
VAT rate	Zakon o PDV BiH (Sl. glasnik BiH 9/2005)	17% standard, 0% exempt — UIO authority	VAT 17% selector

Requirement	Law	Details	Bilko Implementation
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
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
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

Control ID	Description	Type	Applies To	Status
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		

Compliance Overview

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.

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
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)

Data Category	Serbia (RS)	BiH — FBiH	BiH — RS Entity	Croatia (HR)	Legal Basis
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
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)
- 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
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
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 (to be created)
- Terms of Service: ../../legal/TERMS-OF-SERVICE.md (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)

Data Encryption Policy

Data Encryption Policy

> **Project / Organization:** Bilko — Balkan Accounting SaaS **Policy Number:** POL-SEC-ENC-001 **Version:** 1.0 **Date:** 2026-02-23 **Author:** CTO / Security Architect **Status:** Draft **Reviewers:** DPO, Engineering Lead **Classification:** Confidential

Document History

Version	Date	Author	Changes
0.1	2026-02-23	CTO	Initial encryption policy for Bilko accounting SaaS

---

1. Purpose & Scope

This policy defines encryption standards for all data processed by Bilko. Bilko handles regulated financial data across three jurisdictions (Serbia, Bosnia & Herzegovina, Croatia) including tax IDs, IBAN numbers, and financial transaction records that must meet GDPR, ZZPL, and ZZLP BiH requirements.

Scope: All Bilko systems, databases, APIs, backups, and data in transit.

---

2. Data Classification & Encryption Requirements

Level	Label	Examples	Encryption Required

L4-A	Restricted (Personal)	JMBG, OIB	**AES-256-GCM field-level encryption** (prisma-field-encryption) + HMAC-SHA256 hash column + AES-256 at-rest + TLS 1.3 (See ADR-014)
L4-B	Restricted (Business/Financial)	PIB, JIB, IBAN	**AES-256 disk-level encryption** (Railway) + TLS 1.3 + org-scoping + RBAC + API masking for IBAN (last 4 digits in list views) (See ADR-014)
L3	Confidential	Invoice amounts, bank statements, transaction data	**AES-256 at-rest + TLS 1.3**
L2	Internal	Email, name, phone, address	**TLS 1.3** minimum
L1	Public	Organization display name, public invoice ref	No encryption required (but TLS in transit)

---

3. Encryption-in-Transit

Standards

- **Minimum:** TLS 1.2 (legacy client support only)
- **Preferred:** TLS 1.3 — enforced via Cloudflare SSL Full (Strict) mode
- **Cipher suites (TLS 1.3):** TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256
- **Certificate:** Let's Encrypt via Cloudflare (auto-renew) for *.bilko.io
- **HSTS:** `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`

Scope

Connection	Encryption
Browser → Cloudflare	TLS 1.3 (Cloudflare managed)
Cloudflare → Railway API	TLS 1.2+ (Full Strict mode)
API → PostgreSQL (Railway)	`ssl=require` in DATABASE_URL connection string
API → SEF portal (Serbia)	TLS 1.2+ (Serbian government portal)
API → FINA/HR-FISK (Croatia)	TLS 1.2+ (FINA PKI)

Connection	Encryption
API → Sentry	TLS 1.3

What is NOT acceptable

- HTTP (unencrypted) for any Bilko endpoint — Cloudflare redirects HTTP → HTTPS
- Self-signed certificates in production
- TLS 1.0 or TLS 1.1 connections
- Disabling certificate verification in API clients

---

4. Encryption-at-Rest

Database (PostgreSQL on Railway)

- **Algorithm:** AES-256 (Railway managed disk encryption)
- **Level:** Full disk encryption — Railway EU West
- **Backups:** Encrypted using same key before upload to Railway backup storage
- **Connection:** `ssl=require` — plaintext connection not allowed even from same host

Backup Files

- Bilko does not manage its own database backups — Railway handles this
- If manual exports are taken for disaster recovery: encrypt with GPG (AES-256) before storing
- GPG key stored in Vaultwarden, not in same location as backup files

---

5. Field-Level Encryption (L4-A: JMBG and OIB Only)

> **Tiered L4 approach per ADR-014:** Field-level encryption applies ONLY to L4-A personal identifiers (JMBG, OIB). L4-B fields (PIB, JIB, IBAN) rely on disk-level encryption and application controls — see Section 5b. Field-level encryption for publicly available business tax IDs (PIB, JIB) is disproportionate per GDPR Article 32.

Field-level encryption is applied to JMBG and OIB BEFORE writing to the database. The database column stores only ciphertext. The application decrypts on read.

Algorithm

- **Algorithm:** AES-256-GCM (authenticated encryption — provides confidentiality + integrity)
- **IV:** 12 bytes, randomly generated per encryption operation
- **Key:** 32 bytes (256 bits), stored in `FIELD_ENCRYPTION_KEY` environment variable (Railway secret)
- **Output format:** `base64(iv):base64(authTag):base64(ciphertext)` stored as TEXT column

Implementation

```
import { createCipheriv, createDecipheriv, randomBytes } from "crypto";

const ALGORITHM = "aes-256-gcm";

function getKey(): Buffer {
  const hex = process.env.FIELD_ENCRYPTION_KEY;
  if (!hex || hex.length !== 64) {
    throw new Error("FIELD_ENCRYPTION_KEY must be a 64-character hex string (32 bytes)");
  }
  return Buffer.from(hex, "hex");
}

export function encryptField(plaintext: string): string {
  const key = getKey();
  const iv = randomBytes(12);
  const cipher = createCipheriv(ALGORITHM, key, iv);
  const encrypted = Buffer.concat([cipher.update(plaintext, "utf8"), cipher.final()]);
  const authTag = cipher.getAuthTag();
  return [iv, authTag, encrypted].map(b => b.toString("base64")).join(":");
}

export function decryptField(ciphertext: string): string {
  const key = getKey();
  const [ivB64, tagB64, encB64] = ciphertext.split(":");
  const iv = Buffer.from(ivB64, "base64");
  const authTag = Buffer.from(tagB64, "base64");
```

```
  const encrypted = Buffer.from(encB64, "base64");
  const decipher = createDecipheriv(ALGORITHM, key, iv);
  decipher.setAuthTag(authTag);
  return Buffer.concat([decipher.update(encrypted), decipher.final()]).toString("utf8");
}
```

Fields Subject to Field-Level Encryption (L4-A)

Field	Table	Jurisdiction	Notes
`jmbg` (JMBG)	Contact	RS, BA	Serbian/BiH citizen number — irrevocable personal identifier, encodes DOB/gender/region. Stored encrypted + `jmbgHash` HMAC column.
`oib` (OIB)	Contact	HR	Croatian personal/company tax ID — unique cross-system identifier. Stored encrypted + `oibHash` HMAC column.

Fields NOT Subject to Field-Level Encryption (L4-B — Disk-Level + Controls)

Per ADR-014, the following L4 fields are protected by disk-level encryption (Railway AES-256) plus application-layer controls rather than field-level encryption. Field-level encryption for these fields is disproportionate: PIB and JIB are publicly searchable on government registries; IBAN is routinely shared for payment.

Field	Table	Jurisdiction	Controls
`taxId` / `registrationNumber` (PIB)	Contact, Organization	RS	Disk encryption + org-scoping + RBAC + TLS
`taxId` / `registrationNumber` (JIB)	Contact, Organization	BA	Disk encryption + org-scoping + RBAC + TLS
`iban`	BankAccount	All	Disk encryption + org-scoping + RBAC + TLS + API masking (last 4 digits in list views)

Searchability

L4-A encrypted fields (JMBG, OIB) cannot be searched with SQL LIKE or equality. Exact-match lookup uses HMAC hash columns:

1. Store a deterministic HMAC-SHA256 hash in `jmbgHash` / `oibHash` column (separate `FIELD_HMAC_KEY`)
2. Search is performed on the hash column
3. Full plaintext is decrypted only when displaying to an authorized user

---

6. Password Hashing

Parameter	Value
Algorithm	bcrypt
Cost factor	12 (adaptable upward as hardware improves)
Salt	Automatically generated by bcrypt library (16 bytes)
Minimum password entropy	8 chars, 1 uppercase, 1 number, 1 special character
Breach check	HaveIBeenPwned API (k-anonymity — only first 5 chars of SHA1 hash sent)

Never: Store plaintext passwords, use MD5 or SHA1 for passwords, use bcrypt cost factor below 10.

---

7. JWT Signing

Parameter	Value
Algorithm	RS256 (RSA + SHA-256) — asymmetric
Private key	2048-bit RSA, stored in `JWT_PRIVATE_KEY` Railway secret
Public key	Stored in `JWT_PUBLIC_KEY` Railway secret (for verification)
Access token lifetime	15 minutes
Refresh token lifetime	7 days
Key rotation	Annually or on compromise

Why RS256 over HS256: RS256 allows future token verification by external services without sharing the signing secret.

---

8. Monetary Data Integrity

Financial amounts must never be stored as floating-point types due to rounding errors in financial calculations.

Parameter	Standard
Database type	`NUMERIC(19,4)` — PostgreSQL exact decimal
Application type	`Decimal.js` library — not JavaScript `number`
Rounding	Banker's rounding (round half to even)
Currency storage	ISO 4217 code (RSD, BAM, EUR) in separate column

---

9. Key Management Summary

Keys are managed per the Key Management Policy (key-management-policy.md). Encryption keys must never be:

- Committed to source code repositories
- Logged in application logs
- Sent over unencrypted channels
- Stored outside Railway environment variables or Vaultwarden

---

10. Prohibited Algorithms

Algorithm	Status	Reason
MD5	PROHIBITED	Cryptographically broken
SHA-1	PROHIBITED for signing/hashing sensitive data	Collision attacks demonstrated
DES / 3DES	PROHIBITED	Insufficient key length
RC4	PROHIBITED	Multiple vulnerabilities
RSA with key < 2048 bits	PROHIBITED	Insufficient for current threat model
AES-128	PERMITTED (not preferred)	AES-256 required for L4 Restricted data
AES-256-CBC	PERMITTED with caution	GCM preferred (provides authentication)
AES-256-GCM	**REQUIRED** for L4 fields	Authenticated encryption

Approval

Role	Name	Signature	Date
Author	CTO		2026-02-23
Reviewer (DPO)			
Reviewer (Engineering Lead)			
Approver	CEO		

DPIA — Data Protection Impact Assessment

Data Protection Impact Assessment (DPIA)

> **Project:** Bilko — Balkan Accounting SaaS **Version:** 1.0 **Date:** 2026-02-23 **Author:** DPO **Status:** Draft — requires DPO sign-off before launch **Reviewers:** CTO, Legal Counsel, DPO **Classification:** Confidential

Document History

Version	Date	Author	Changes
0.1	2026-02-23	DPO	Initial DPIA for Bilko accounting SaaS

---

1. DPIA Necessity Assessment

Is this DPIA mandatory? YES.

Bilko meets multiple high-risk criteria under GDPR Article 35 and equivalent provisions in ZZPL (Serbia Art. 54) and ZZLP BiH (Art. 17a):

Criterion	Applies	Reason
Large-scale processing of sensitive data	YES	Tax IDs (PIB, JMBG, OIB, JIB) qualify as identification data processed at scale
Systematic processing of personal data	YES	Core business function — every user's financial data processed continuously

Criterion	Applies	Reason
Processing that determines access to financial services	YES	Accounting data used for tax filings, credit applications, regulatory compliance
Multi-jurisdictional cross-border transfers	YES	RS/BA to EU host (Railway)
Vulnerable data subjects	PARTIAL	Some SMB owners may be natural persons with limited tech literacy

---

2. System Description

System Name: Bilko Cloud Accounting Platform **Controller:** Bilko d.o.o. / Bilko d.o.o. Sarajevo / Bilko d.o.o. Zagreb (per jurisdiction) **Processor(s):** Railway (hosting), Cloudflare (CDN/WAF), Sentry (error tracking) **DPO Contact:** dpo@bilko.io

Purpose: Provide cloud-based double-entry accounting, invoicing, expense tracking, VAT reporting, and e-invoicing integration (SEF for RS, HR-FISK for HR) to SMBs in Serbia, Bosnia & Herzegovina, and Croatia.

Lawful basis: Contract performance (Art. 6(1)(b)) for core accounting services; Legal obligation (Art. 6(1)(c)) for tax ID storage and retention periods.

---

3. Data Flows

```
flowchart LR
    subgraph USERS["Data Subjects"]
        OWNER["Business Owner\n(natural person)"]
        CLIENT["Client (Contact)\n(natural person or legal entity)"]
    end

    subgraph BILKO["Bilko Platform"]
        API["Express API\n(Railway EU West)"]
        DB["PostgreSQL\n(Railway EU West)"]
        AUDIT["LoggedAction\nAudit Table"]
    end

    subgraph EXTERNAL["External Integrations"]
```

```
        SEF["SEF Portal\n(Serbia — efaktura.mfin.gov.rs)"]
        HRFISK["HR-FISK\n(Croatia — FINA)"]
        CF["Cloudflare WAF"]
        SENTRY["Sentry\n(Error tracking)"]
    end

    OWNER -->|"Creates account\nEmail, name, OrgPIB"| API
    OWNER -->|"Creates invoice\nBuyer PIB/OIB/JIB/JMBG\nIBAN\nAmounts"| API
    CLIENT -->|"Receives invoice\n(email)"| OWNER
    API --> DB
    API --> AUDIT
    API -->|"e-invoice XML"| SEF
    API -->|"e-invoice XML + FINA cert"| HRFISK
    API -->|"All traffic"| CF
    API -->|"Error traces"| SENTRY
```

Data Inventory

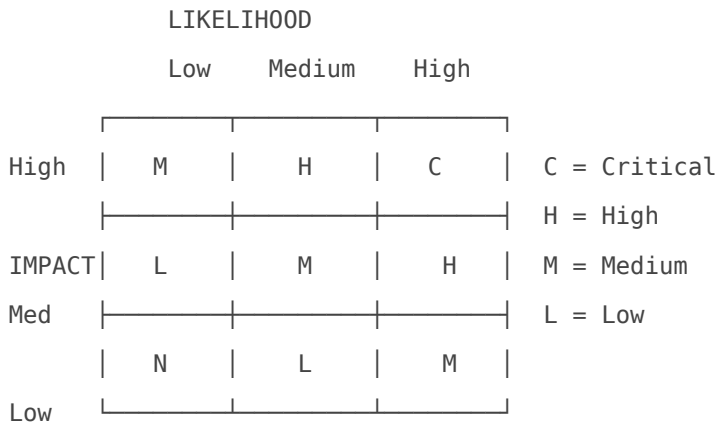
Data Element	Source	Stored	Encrypted	Retention	Jurisdiction
Email address	User registration	YES	No (indexed)	Account lifetime	All
Full name	User registration	YES	No	Account lifetime	All
Organization name	Registration	YES	No	10-11 years	All
PIB (Serbia tax ID)	Invoice creation	YES	**Disk encryption + API controls** (L4-B, See ADR-014)	10 years	RS
JMBG (Serbia personal ID)	Invoice — natural persons	YES	**AES-256-GCM field-level** + HMAC-SHA256 hash (L4-A, See ADR-014)	10 years	RS
OIB (Croatia personal tax ID)	Invoice creation	YES	**AES-256-GCM field-level** + HMAC-SHA256 hash (L4-A, See ADR-014)	11 years	HR
JIB (BiH tax ID)	Invoice creation	YES	**Disk encryption + API controls** (L4-B, See ADR-014)	10-11 years	BA

Data Element	Source	Stored	Encrypted	Retention	Jurisdiction
IBAN	Bank accounts / invoices	YES	**Disk encryption + API masking** (last 4 digits in list views) (L4-B, See ADR-014)	10-11 years	All
Invoice amounts	Invoices	YES	No (NUMERIC 19,4)	10-11 years	All
IP address	Session logs	YES	No	30 days	All
Browser user agent	Session logs	YES	No	30 days	All
Audit trail entries	System	YES	No	10-11 years	All

---

4. Risk Assessment

Risk Matrix



Identified Risks

Risk ID	Risk	Impact	Likelihood	Rating	Mitigation
R-01	Unauthorized access to personal IDs (JMBG/OIB)	High	Medium	**H**	AES-256-GCM field-level encryption (L4-A, ADR-014); RBAC restricts access

Risk ID	Risk	Impact	Likelihood	Rating	Mitigation
R-01b	Unauthorized access to business IDs (PIB/JIB)	Low-Medium	Medium	**M**	Disk encryption + org-scoping + RBAC (L4-B, ADR-014); PIB/JIB are publicly available on gov portals
R-02	Cross-tenant data leak (one org sees another's data)	High	Low	**M**	Prisma org-scoped WHERE on every query; automated test suite
R-03	IBAN exposure enabling financial fraud	Medium	Low	**L**	Disk encryption + API masking (last 4 digits in list views) (L4-B, ADR-014); IBAN is routinely shared for payment
R-04	Breach of invoice data (amounts, buyer/seller details)	High	Low	**M**	TLS 1.3; Railway AES-256 at rest; RBAC
R-05	Railway data center compromise	High	Very Low	**L**	Railway EU West (ISO 27001); DPA signed; encrypted backups
R-06	Insufficient retention — legal/regulatory penalty	High	Medium	**H**	Retention lock prevents deletion; automated alerts before expiry
R-07	Failed SEF/HR-FISK e-invoice — business disruption + fine	High	Medium	**H**	Test environment; idempotent submission; alert on failure
R-08	Employee/insider access to client financial data	Medium	Low	**L**	RBAC; LoggedAction audit trail; background checks for staff
R-09	Account takeover via credential stuffing	High	Medium	**H**	bcrypt 12; rate limiting 5/15min auth; HIBP breach check

Risk ID	Risk	Impact	Likelihood	Rating	Mitigation
R-10	JMBG processed without adequate legal basis	High	Low	**M**	JMBG only accepted when user confirms natural person billing
R-11	Cross-border transfer BA → Railway without adequate mechanism	Medium	Medium	**M**	Standard Contractual Clauses with Railway for BiH users

Residual Risk Assessment

After applying controls in Section 5:

- R-01 (JMBG/OIB): Residual = **Low** (AES-256-GCM field-level encryption + RBAC, ADR-014 Tier 1)
- R-01b (PIB/JIB): Residual = **Low** (disk encryption + org-scoping; data is publicly available on gov registries)
- R-03 (IBAN): Residual = **Low** (disk encryption + API masking; IBAN is routinely shared for payment)
- R-06, R-07, R-09: Residual = **Medium** (operational dependencies remain)
- R-11: Residual = **Low** (SCC in place)

Overall residual risk: MEDIUM — Acceptable with DPO sign-off.

---

5. Mitigation Measures

Control	Addresses	Implementation
AES-256-GCM field-level encryption for JMBG and OIB (L4-A)	R-01, R-10	`prisma-field-encryption` extension — `jmbg` and `oib` fields encrypted before write; `jmbgHash` / `oibHash` HMAC columns for exact-match lookup (See ADR-014)
Disk-level encryption + API controls for PIB, JIB, IBAN (L4-B)	R-01b, R-03	Railway AES-256 disk encryption + org-scoping + RBAC; IBAN masked to last 4 digits in list responses (See ADR-014)
Org-scoped WHERE on all Prisma queries	R-02	Lint rule + automated isolation tests
JWT 15min access + 7day refresh + rotation	R-09	Express auth middleware

Control	Addresses	Implementation
bcrypt cost factor 12	R-09	Password hashing on registration
Rate limiting: 5 auth req / 15min	R-09	`express-rate-limit`
HIBP breach check on registration	R-09	k-anonymity API call
LoggedAction audit trail (append-only)	R-08	Prisma middleware — every write operation
Retention lock (10-11yr minimum)	R-06	`deletedAt` check + age validation before hard delete
DPA with Railway	R-05	Legal — sign before launch
SCCs with Railway (for BiH users)	R-11	Legal — sign before launch
SEF/HR-FISK idempotent submission + retry	R-07	API integration with deduplication key
JMBG consent gate	R-10	UI checkbox: "This invoice is for a natural person"

---

6. Consultation

DPO Consultation

- DPO: dpo@bilko.io
- DPIA mandatory per GDPR Art. 35 — DPO must be consulted before processing begins
- DPO opinion: [PENDING]

Supervisory Authority Prior Consultation

Prior consultation required if residual risk remains HIGH after all mitigations. Current assessment: MEDIUM — **prior consultation NOT required**, but this must be reasserted when HR-FISK and JMBG features are fully implemented.

Data Subject Consultation

Consideration: SMB owners are sophisticated business users. DPIA does not require data subject consultation for B2B accounting software, but privacy policy must clearly explain tax ID processing.

---

7. Approval & Review

DPO Sign-off Required Before: Any feature that processes PIB, JMBG, OIB, JIB, or IBAN goes to production.

Next DPIA Review: When adding new data categories, new jurisdictions, or new external integrations.

Role	Name	Signature	Date
Author	DPO		2026-02-23
Reviewer (CTO)			
DPO Approval			
CEO Sign-off			

Key Management Policy

Key Management Policy

> **Organization:** Bilko — Balkan Accounting SaaS **Policy Number:** POL-SEC-KM-001 **Version:** 1.0 **Date:** 2026-02-23 **Author:** CTO **Status:** Draft **Reviewers:** DPO, Engineering Lead **Classification:** Confidential — Restricted

Document History

Version	Date	Author	Changes
0.1	2026-02-23	CTO	Initial key management policy for Bilko

---

1. Purpose & Scope

This policy defines the lifecycle management for all cryptographic keys and secrets used by Bilko. It covers key generation, storage, rotation, revocation, and destruction.

Scope: All Bilko production and staging environments. All personnel with access to Railway environment variables or Vaultwarden.

---

2. Key Inventory

Key ID	Key Type	Purpose	Storage	Rotation Period	Owner
JWT_PRIVATE_KEY	RSA 2048-bit private key	JWT access token signing (RS256)	Railway secret (production)	Annual	CTO
JWT_PUBLIC_KEY	RSA 2048-bit public key	JWT access token verification	Railway secret (production)	Annual (with private)	CTO
REFRESH_TOKEN_SECRET	64-byte random hex	Refresh token HMAC signing	Railway secret	Annual	CTO

Key ID	Key Type	Purpose	Storage	Rotation Period	Owner
FIELD_ENCRYPTION_KEY	32-byte random hex (AES-256)	Field-level encryption of PIB/JMBG/OIB/JIB/IBAN	Railway secret	Annual	CTO
FIELD_HMAC_KEY	32-byte random hex	Deterministic HMAC for searchable hash on encrypted fields	Railway secret	Annual (with FIELD_ENCRYPTION_KEY)	CTO
DATABASE_URL	PostgreSQL connection string with credentials	Database access	Railway secret	On compromise / quarterly review	CTO
SEF_API_KEY	API key string	Serbia SEF e-invoice portal (per org)	DB (encrypted) per org	Per SEF portal policy	Per organization
FINA_CERT	X.509 certificate + private key	HR-FISK e-invoice signing (FINA PKI)	DB (encrypted) per org	Per FINA PKI (1-3 years)	Per organization
SENTRY_DSN	DSN string	Error tracking	Railway secret / env var	On compromise	CTO

---

3. Key Hierarchy

```
graph TD
    ROOT["Root Secrets\n(CTO personal Vaultwarden vault)"]
    RAILWAY["Railway Environment Secrets\n(production / staging / dev)"]
    ORG_SECRETS["Per-Organization Secrets\n(DB encrypted, L4 Restricted)\nSEF API keys, FINA certs"]
    APP["Application Runtime\n(keys loaded from env at startup)"]

    ROOT -->|"Provision"| RAILWAY
    RAILWAY -->|"Load at boot"| APP
    ROOT -->|"Rotation authority"| ORG_SECRETS
    ORG_SECRETS -->|"Decrypt on request"| APP
```

Principle: No key material is ever committed to source code. No key is stored in plaintext outside Railway secrets or Vaultwarden.

---

4. Key Generation Standards

Key Type	Generation Method	Entropy Requirements
RSA (JWT)	`openssl genrsa 2048`	2048-bit minimum
Symmetric (AES-256)	`openssl rand -hex 32`	256 bits (32 bytes)
HMAC key	`openssl rand -hex 32`	256 bits
Refresh token secret	`openssl rand -hex 64`	512 bits
API keys (external)	Generated by external portal (SEF/FINA)	Per external system

Commands:

```
# Generate JWT key pair
openssl genrsa -out jwt_private.pem 2048
openssl rsa -in jwt_private.pem -pubout -out jwt_public.pem

# Generate AES-256 field encryption key
openssl rand -hex 32

# Generate HMAC key
openssl rand -hex 32
```

All generated keys must be imported to Railway and Vaultwarden within 1 hour. Local files deleted securely after import.

---

5. Key Storage

Production Keys (Railway)

- All production keys stored as Railway environment variables
- Railway EU West region — encrypted at rest by Railway (AES-256)
- Access: CTO + one designated backup (CEO) only
- Two-factor authentication mandatory for Railway account
- Railway account uses ALAI SSO / strong password (≥20 chars, in Vaultwarden)

Staging/Dev Keys

- Separate Railway project (staging) — different keys from production
- Dev: `.env.local` files excluded from git via `.gitignore`
- Dev keys may use weaker entropy but must still be valid format

Vaultwarden (Backup & Documentation)

- URL: https://vault.basicconsulting.no
- Stores: production key material as secure notes (encrypted)
- Access: CTO + CEO (break-glass access)
- Purpose: Recovery if Railway secrets are lost; rotation documentation

Per-Organization Secrets (SEF API Keys, FINA Certificates)

- Stored in PostgreSQL `OrganizationSecret` table
- Value encrypted with FIELD_ENCRYPTION_KEY before storage
- Decrypted in-memory only when needed for API call
- FINA private keys additionally protected with password (stored separately)

---

6. Key Rotation Procedures

6.1 Annual Rotation (Standard)

Schedule: First Monday of each calendar year.

FIELD_ENCRYPTION_KEY rotation (most sensitive — requires re-encryption):

```
1. Generate new FIELD_ENCRYPTION_KEY (openssl rand -hex 32)
2. Deploy a migration job that:
   a. Reads each encrypted field with old key
   b. Decrypts
   c. Re-encrypts with new key
   d. Writes back to DB
3. Migration must be atomic per record (read old → write new in transaction)
4. Only after 100% migration: update Railway secret to new key
5. Delete old key from Vaultwarden (add to archive note with date)
6. Test: attempt decryption with both old (should fail) and new (should succeed) keys
```

JWT key pair rotation (zero-downtime):

```
1. Generate new RSA key pair
2. Add new public key to JWKS endpoint alongside old (support both during rotation window)
```

```
3. Begin issuing new tokens signed with new private key
4. Wait for all old tokens to expire (15 minutes max)
5. Remove old public key from JWKS
6. Update JWT_PRIVATE_KEY and JWT_PUBLIC_KEY in Railway
7. Invalidate all refresh tokens (users will re-login)
```

6.2 Emergency Rotation (On Compromise)

If a key is suspected compromised:

1. **Immediately** invalidate: all user sessions (clear RefreshToken table)
2. Generate new key within 15 minutes
3. Update Railway secret
4. Deploy new application instance (Railway auto-deploys on env var change)
5. Document in Vaultwarden: old key, date of compromise, date of rotation
6. Assess whether breach notification is required (see data-breach-response-plan.md)

6.3 FINA Certificate (HR-FISK) Rotation

FINA X.509 certificates for HR-FISK e-invoicing have a defined validity period (1-3 years per FINA PKI).

```
1. FINA certificate expiry alert fires 60 days before expiry
2. Organization admin is notified to renew via FINA portal
3. New certificate uploaded through Bilko settings → HR eRačun → Certificate
4. Old certificate archived (not deleted — needed to verify past submissions)
5. Test: submit a test e-invoice via HR-FISK test environment with new certificate
```

---

7. Key Access Control

Key	Who Can Access	How
JWT_PRIVATE_KEY	Application only (Railway env)	Never exposed via API; loaded at startup
FIELD_ENCRYPTION_KEY	Application only	Never logged; never returned in API response
DATABASE_URL	Application + CTO	Railway secret; CTO can view in Railway dashboard
SEF API keys	Application + org owner	Decrypted only for SEF API calls; org owner can rotate via settings

Key	Who Can Access	How
FINA certificates	Application + org owner	Decrypted only for HR-FISK submissions

Access log: All Railway secret views logged in Railway audit trail. Any access outside normal deployment is reviewed by CTO.

---

8. Escrow & Recovery

FIELD_ENCRYPTION_KEY Escrow (Critical)

The FIELD_ENCRYPTION_KEY is the most critical key — loss means permanent loss of all L4 Restricted field data (tax IDs, IBAN).

Escrow procedure:

- FIELD_ENCRYPTION_KEY stored in Vaultwarden secure note accessible to: CTO, CEO
- Vaultwarden has its own backup (see system infrastructure docs)
- Key material noted with: creation date, rotation date, description

If FIELD_ENCRYPTION_KEY is lost and not recoverable: All encrypted field data is permanently unreadable. This is a catastrophic data loss event. Contact legal counsel and affected supervisory authorities.

Railway Account Recovery

- Railway root account: admin@bilko.io (password in Vaultwarden)
- 2FA recovery codes: Vaultwarden secure note
- Designated backup access: CEO has view access to Railway (read-only)

---

9. Key Destruction

When a key is retired (superseded by rotation):

1. Remove from Railway environment variables
2. Remove from active Vaultwarden entries
3. Archive to Vaultwarden secure note: "Retired Keys" with date and reason
4. Old FIELD_ENCRYPTION_KEY versions: retained for 3 months after rotation (in case rollback needed), then permanently deleted from Vaultwarden

Approval

Role	Name	Signature	Date
Author	CTO		2026-02-23
Reviewer (DPO)			
Reviewer (Engineering Lead)			
Approver	CEO		

Breach Response Plan

Data Breach Response Plan

> **Organization:** Bilko — Balkan Accounting SaaS **Document Number:** IRP-SEC-001 **Version:** 1.0 **Date:** 2026-02-23 **Author:** DPO / CTO **Status:** Draft — requires DPO approval before launch **Reviewers:** CTO, DPO, CEO **Classification:** Confidential

Document History

Version	Date	Author	Changes
0.1	2026-02-23	DPO	Initial breach response plan — three-jurisdiction (RS, BA, HR)

---

1. Incident Response Team

Role	Person	Contact	Responsibility
Incident Commander	CTO	cto@bilko.io	Technical response, containment, investigation
DPO	DPO	dpo@bilko.io	Regulatory notification, data subject communication
CEO	CEO	ceo@bilko.io	Stakeholder comms, business decisions, media
Legal Counsel	External	legal@bilko.io	Regulatory advice, notification drafting
On-call Engineer	Rotates	Slack: #bilko-incidents	First responder — detection, initial containment

Escalation order: On-call → CTO → DPO → CEO

2. What Constitutes a Breach

A personal data breach is any security incident leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Examples

Incident	Breach?	Severity
Unauthorized access to a customer's invoice data	YES	HIGH
Exposure of PIB/JMBG/OIB/JIB tax IDs	YES	CRITICAL
IBAN numbers exposed	YES	CRITICAL
Railway DB credentials exposed	YES — potential breach	CRITICAL
Server error logs contain email addresses	YES (minor)	LOW
Employee accidentally emails invoice to wrong address	YES	MEDIUM
Unsuccessful SQL injection attempt (no data accessed)	NO — log and monitor	LOW
DDoS attack — service unavailable, no data accessed	NO	N/A

3. Response Timeline

```
timeline
    title Breach Response Timeline (72 hours)
    section Hour 0
        Detection : Alert fires (monitoring, customer report, employee discovery)
        Verification : Is this a real breach? Contain false positives.
    section Hour 1-4
        Containment : Block attacker, revoke credentials, isolate affected systems
        Assessment : What data was accessed? How many records? Which jurisdictions?
    section Hour 4-24
        Investigation : Root cause analysis. Audit logs (LoggedAction table).
        Internal notification : CTO, DPO, CEO briefed.
```

```
    section Hour 24-48
        Regulatory notification : Poverenik (RS), AZLP (BA), AZOP (HR) if required
        Evidence preservation : Immutable audit trail extracted. Logs archived.
    section Hour 48-72
        Data subject notification : If high risk to individuals
        Remediation : Patch deployed. Controls improved.
    section After 72h
        Post-mortem : Root cause documented. Prevention measures implemented.
        Follow-up reporting : Supervisory authorities updated if required.
```

---

4. Regulatory Notification Requirements

4.1 Notification Thresholds

Jurisdiction	Law	Notify Authority	Deadline	Condition
Croatia	GDPR Art. 33	AZOP (azop.hr)	**72 hours**	Unless breach is unlikely to result in risk to rights/freedoms
Serbia	ZZPL Art. 56	Poverenik (poverenik.rs)	**72 hours**	Applies analogously (GDPR-aligned law)
Bosnia & Herzegovina	ZZLP BiH Art. 20	AZLP (azlp.gov.ba)	**Best practice 72 hours** (law less specific)	Recommended to align with GDPR practice

Default: Notify all three authorities unless legal counsel advises otherwise.

4.2 Authority Contact Details

Authority	Jurisdiction	Website	Notification Method
Agencija za zaštitu osobnih podataka (AZOP)	Croatia	azop.hr	Online form + email: azop@azop.hr
Poverenik za informacije od javnog značaja	Serbia	poverenik.rs	Online form at poverenik.rs/zastitapodataka
Agencija za zaštitu ličnih podataka (AZLP)	Bosnia & Herzegovina	azlp.gov.ba	Email: azlp@azlp.gov.ba

4.3 Notification Content (per GDPR Art. 33 / ZZPL Art. 56)

Required information for supervisory authority notification:

```
1. Nature of the breach (what happened, how discovered)
2. Categories and approximate number of data subjects affected
3. Categories and approximate number of records affected
4. Contact details of DPO: dpo@bilko.io
5. Likely consequences of the breach
6. Measures taken or proposed to address the breach
```

Template: See Section 7.1

4.4 Data Subject Notification (GDPR Art. 34)

Notify affected individuals "without undue delay" if breach is **likely to result in high risk** to their rights and freedoms.

High risk triggers for Bilko data:

- Tax ID (PIB/JMBG/OIB/JIB) exposure — identity theft risk
- IBAN exposure — financial fraud risk
- Full invoice data exposure — business espionage risk

---

5. Response Procedures

5.1 Detection & Verification (0–1 hour)

Detection sources:

- Sentry error tracking — unusual error patterns
- Railway logs — unexpected query volumes or failed auth attempts
- Cloudflare WAF alerts — unusual traffic patterns
- Customer complaint — "I can see another company's data"
- Employee discovery

Verification steps:

1. Access Railway logs and Cloudflare analytics

2. Query LoggedAction table for anomalous access patterns:

```
SELECT userId, orgId, action, tableName, ipAddress, COUNT(*)
FROM "LoggedAction"
WHERE timestamp > NOW() - INTERVAL '1 hour'
GROUP BY userId, orgId, action, tableName, ipAddress
ORDER BY COUNT(*) DESC;
```

3. Confirm whether actual personal data was accessed (not just attempted)
4. Declare incident: `#bilko-incidents` Slack channel + page Incident Commander

5.2 Containment (1–4 hours)

Immediate actions (within 30 minutes of confirmation):

- ☐ Revoke affected user sessions (invalidate JWT refresh tokens in DB)
- ☐ If credentials compromised: rotate all Railway environment secrets
- ☐ If SQL injection: enable Railway maintenance mode temporarily
- ☐ If insider threat: suspend user account, preserve audit logs
- ☐ If third-party compromise: revoke API keys to SEF/FINA/Sentry

Preserve evidence:

- Extract relevant LoggedAction rows to immutable storage (S3 / local encrypted archive) before any system changes
- Do not delete logs, rotate secrets in place (old secret documented in Vaultwarden with timestamp)

5.3 Assessment (4–24 hours)

Determine scope:

- Which organizations were affected?
- Which data categories? (check against Data Inventory in DPIA)
- Approximate number of data subjects?
- Which jurisdictions? (RS, BA, HR, or all?)
- Was data exfiltrated, or only accessed?
- What is the risk to data subjects?

Severity classification:

Severity	Criteria	Response

CRITICAL	Tax IDs, IBAN, financial amounts exfiltrated	Notify all authorities within 24h; notify all affected data subjects
HIGH	Invoice metadata accessed across tenant boundary	Notify authorities within 72h; assess individual notification
MEDIUM	Email/name exposure, no financial data	Notify authorities if >250 records; assess individual notification
LOW	Single record, no sensitive data, no exfiltration	Document internally; no mandatory notification

5.4 Regulatory Notification (24–72 hours)

1. DPO drafts notification using template in Section 7.1
2. Legal counsel reviews
3. CEO approves
4. DPO submits to AZOP (HR), Poverenik (RS), AZLP (BA) simultaneously
5. Log submission timestamp and reference numbers received

If full details not available within 72 hours: Submit initial notification with known information and state investigation is ongoing. Supplement with additional notifications as information becomes available (GDPR Art. 33(4) allows phased notification).

5.5 Data Subject Notification

If high risk determined (Section 4.4):

1. Identify email addresses of all affected data subjects
2. DPO drafts data subject notification (see Section 7.2)
3. Send via Bilko email account — do not use marketing email tools
4. Provide clear guidance on what to do (change password, monitor bank statements)

---

6. Post-Incident

6.1 Post-Mortem

Complete within 2 weeks of incident resolution. Template: `OPERATIONS/post-mortem.md`

- Root cause (5 Whys)
- Timeline reconstruction from LoggedAction + logs
- What controls failed?
- What controls worked?

- Action items with owners and deadlines

6.2 Regulatory Follow-Up

- AZOP, Poverenik, AZLP may request follow-up information within 3 months
- Maintain incident dossier for minimum 3 years (GDPR Art. 33(5))
- Document: what happened, who was notified, when, remediation taken

6.3 Insurance

- Notify cyber insurance provider if breach exceeds threshold (per policy)
- Preserve evidence for potential claims

---

7. Notification Templates

7.1 Supervisory Authority Notification (English — adapt per jurisdiction)

```
Subject: Personal Data Breach Notification — Bilko Cloud Accounting — [DATE]

To: [AZOP / Poverenik / AZLP]

We are reporting a personal data breach pursuant to [GDPR Art. 33 / ZZPL Art. 56 / ZZLP BiH Art. 20].

Controller: Bilko d.o.o. | dpo@bilko.io | +[phone]
DPO Contact: dpo@bilko.io

1. NATURE OF BREACH
[Description: what happened, when discovered, how]

2. DATA SUBJECTS AFFECTED
Approximate number: [NUMBER]
Categories: [accountants / business owners / invoice recipients]

3. RECORDS AFFECTED
Categories: [tax IDs / IBAN / invoice amounts / email addresses]
```

```
Approximate number: [NUMBER]

4. LIKELY CONSEQUENCES
[Identity theft risk / financial fraud risk / business espionage risk]

5. MEASURES TAKEN
[Containment steps, credential rotation, patch deployed]
[Ongoing investigation]

6. FURTHER INFORMATION
This notification is [complete / preliminary – further information to follow].

[DPO Name]
DPO – Bilko
dpo@bilko.io
```

7.2 Data Subject Notification (Croatian — adapt for RS/BA)

```
Predmet: Obavijest o povredi osobnih podataka – Bilko

Poštovani/a,

Obavještavamo Vas da je Bilko bio izložen sigurnosnom incidentu koji je mogao
utjecati na Vaše osobne podatke.

Što se dogodilo:
[Jednostavan opis – kada, što je bilo pristupljeno]

Koji su Vaši podaci bili zahvaćeni:
[Navesti konkretno: PIB, IBAN, iznosi računa – samo što je relevantno]

Što smo poduzeli:
[Koraci: blokiranje pristupa, obavještavanje AZOP-a, poboljšanje sigurnosti]

Što možete učiniti:
- Promijenite lozinku na bilko.io
- Pratite aktivnosti na bankovnim računima
- Kontaktirajte nas na dpo@bilko.io s pitanjima
```

```
Izvinjenje:
Žao nam je što se ovo dogodilo. Zaštita Vaših podataka naša je prioritetna obveza.

S poštovanjem,
Bilko tim
dpo@bilko.io
```

Approval

Role	Name	Signature	Date
Author	DPO / CTO		2026-02-23
Reviewer (CEO)			
DPO Approval			
Legal Counsel Approval			

Security Testing Policy

Security Testing Policy

> **Organization:** Bilko — Balkan Accounting SaaS **Policy Number:** POL-SEC-TEST-001 **Version:** 1.0 **Date:** 2026-02-23 **Author:** CTO / Security Engineer **Status:** Draft **Reviewers:** Engineering Lead, DPO **Classification:** Confidential

Document History

Version	Date	Author	Changes
0.1	2026-02-23	CTO	Initial security testing policy for Bilko

---

1. Purpose & Scope

This policy defines the security testing requirements, tools, schedule, and acceptance criteria for the Bilko platform. Bilko handles regulated financial data (tax IDs, IBAN, accounting records) across three jurisdictions. Security testing is mandatory, not optional.

Scope: All Bilko applications — Express API (`apps/api/`), Next.js frontend (`apps/web/`), database layer (Prisma + PostgreSQL), and external integrations (SEF, HR-FISK).

---

2. Security Testing Pyramid

```
graph TD
    subgraph AUTOMATED["Automated (runs every CI pipeline)"]
        SAST["SAST\nESLint Security Rules\nTypeScript strict mode\nnpm audit\nSnyk SCA"]
        UNIT["Security Unit Tests\nVitest\nRBAC matrix tests\nOrg isolation tests\nEncryption tests\nVAT accuracy tests"]
        INT["Integration Tests\nVitest + Supertest\nAuth flow tests\nJWT validation\nRate
```

```
limiting tests"]
    end

    subgraph PERIODIC["Periodic (scheduled)"]
        DAST["DAST\nOWASP ZAP\nMonthly + pre-release"]
        E2E["Security E2E\nPlaywright\nCross-tenant boundary tests\nPrivilege escalation
tests"]
    end

    subgraph MANUAL["Manual (scheduled)"]
        PENTEST["Penetration Test\nExternal vendor\nAnnual"]
        REVIEW["Security Code Review\nPre-merge (security-sensitive PRs)\nArchitecture review
quarterly"]
    end

    UNIT --> INT --> DAST --> PENTEST
```

---

3. Automated Security Testing (CI/CD)

Every push to `main` and every pull request triggers:

3.1 Static Analysis (SAST)

Tool	What It Checks	Failure Threshold
ESLint + `eslint-plugin-security`	Common JS security patterns (eval, RegExp DoS, object injection)	Any `error` level finding blocks merge
TypeScript strict mode	Type safety prevents implicit `any` that could bypass validation	Build failure blocks merge
`npm audit --audit-level=high`	Known vulnerabilities in dependencies	HIGH or CRITICAL CVEs block merge
Snyk (optional Phase 2)	Deeper SCA including license compliance	CRITICAL blocks merge

3.2 Security Unit Tests (Vitest)

Location: `apps/api/src/__tests__/security/`

Required test suites:

RBAC Matrix Tests

```
// Every permission combination must be explicitly tested
describe("RBAC — Invoice access", () => {
  const roles = ["owner", "admin", "accountant", "viewer"];

  test.each([
    ["owner", "create", true],
    ["admin", "create", true],
    ["accountant", "create", true],
    ["viewer", "create", false],
    ["owner", "delete", true],
    ["admin", "delete", true],
    ["accountant", "delete", false],
    ["viewer", "delete", false],
  ])("role=%s action=%s expected=%s", async (role, action, expected) => {
    const token = signTestJWT({ role, org: "org-1" });
    const res = await request(app)
      .post(`/api/invoices`)
      .set("Authorization", `Bearer ${token}`);
    // check response matches expected
  });
});
```

Organization Isolation Tests (Multi-Tenant Critical)

```
describe("Org isolation — no cross-tenant data leak", () => {
  let org1Token: string;
  let org2InvoiceId: string;

  beforeAll(async () => {
    // Setup two orgs with data
    org1Token = signTestJWT({ org: "org-1", role: "owner" });
    const org2Token = signTestJWT({ org: "org-2", role: "owner" });

    // Create invoice in org-2
    const res = await request(app)
      .post("/api/invoices")
      .set("Authorization", `Bearer ${org2Token}`)
      .send(validInvoicePayload);
```

```
    org2InvoiceId = res.body.id;
  });

  test("org-1 cannot read org-2 invoice", async () => {
    const res = await request(app)
      .get(`/api/invoices/${org2InvoiceId}`)
      .set("Authorization", `Bearer ${org1Token}`);
    expect(res.status).toBe(404); // NOT 403 — don't reveal existence
  });

  test("org-1 list does not include org-2 data", async () => {
    const res = await request(app)
      .get("/api/invoices")
      .set("Authorization", `Bearer ${org1Token}`);
    const ids = res.body.data.map((i: any) => i.id);
    expect(ids).not.toContain(org2InvoiceId);
  });
});
```

Field Encryption Tests

```
describe("Field encryption — L4 Restricted", () => {
  test("PIB stored encrypted in DB", async () => {
    const testPIB = "123456789"; // fake PIB
    // Create contact with PIB
    await request(app)
      .post("/api/contacts")
      .set("Authorization", `Bearer ${ownerToken}`)
      .send({ name: "Test", taxId: testPIB, type: "RS" });

    // Read raw DB value — should not be plaintext
    const raw = await prisma.$queryRaw`
      SELECT "taxId" FROM "Contact" WHERE name = 'Test'
    `;
    expect(raw[0].taxId).not.toBe(testPIB);
    expect(raw[0].taxId).toMatch(/^[A-Za-z0-9+/]+=*:[A-Za-z0-9+/]+=*:[A-Za-z0-9+/]+=*$/);
    // Should be base64:base64:base64 format (iv:authTag:ciphertext)
  });

  test("decrypted PIB matches original on read", async () => {
```

```
    const res = await request(app)
      .get("/api/contacts")
      .set("Authorization", `Bearer ${ownerToken}`);
    const contact = res.body.data.find((c: any) => c.name === "Test");
    expect(contact.taxId).toBe("123456789");
  });
});
```

VAT Accuracy Tests (Financial Compliance)

```
describe("VAT calculation accuracy", () => {
  test("RS: VAT 20% on standard goods (NUMERIC precision)", () => {
    const net = new Decimal("100.00");
    const vatAmount = net.mul("0.20");
    const gross = net.plus(vatAmount);
    expect(vatAmount.toString()).toBe("20.00");
    expect(gross.toString()).toBe("120.00");
  });

  test("HR: VAT 25% (EUR since Jan 2024)", () => {
    const net = new Decimal("100.00");
    const gross = net.mul("1.25");
    expect(gross.toString()).toBe("125.00");
  });

  test("BA: VAT 17% (UIO standard)", () => {
    const net = new Decimal("100.00");
    const gross = net.mul("1.17");
    expect(gross.toString()).toBe("117.00");
  });

  test("No float drift on invoice totals", () => {
    // Known JS float bug: 0.1 + 0.2 !== 0.3
    const line1 = new Decimal("0.10");
    const line2 = new Decimal("0.20");
    expect(line1.plus(line2).toString()).toBe("0.30");
    // Contrast: expect(0.1 + 0.2).toBe(0.3) would FAIL
  });
});
```

Authentication Tests

```
describe("Auth — JWT security", () => {
  test("expired access token returns 401", async () => {
    const expiredToken = signTestJWT({ exp: Math.floor(Date.now()/1000) - 1 });
    const res = await request(app)
      .get("/api/invoices")
      .set("Authorization", `Bearer ${expiredToken}`);
    expect(res.status).toBe(401);
  });

  test("tampered token returns 401", async () => {
    const validToken = signTestJWT({ role: "viewer" });
    // Tamper: change role claim in payload
    const parts = validToken.split(".");
    const payload = JSON.parse(Buffer.from(parts[1], "base64url").toString());
    payload.role = "owner"; // attempt privilege escalation
    parts[1] = Buffer.from(JSON.stringify(payload)).toString("base64url");
    const tamperedToken = parts.join(".");
    const res = await request(app)
      .delete("/api/invoices/any-id")
      .set("Authorization", `Bearer ${tamperedToken}`);
    expect(res.status).toBe(401);
  });

  test("rate limiting: 6th auth attempt in 15min returns 429", async () => {
    for (let i = 0; i < 5; i++) {
      await request(app).post("/api/auth/login").send({ email: "x", password: "wrong" });
    }
    const res = await request(app).post("/api/auth/login").send({ email: "x", password:
"wrong" });
    expect(res.status).toBe(429);
  });
});
```

3.3 Dependency Scanning

```
# .github/workflows/security.yml
- name: Audit dependencies
  run: npm audit --audit-level=high
  # HIGH or CRITICAL CVEs fail the build
```

```
- name: Check for secrets in code
  uses: trufflesecurity/trufflehog@main
  # Scans for committed credentials, API keys
```

Dependency update policy:

- CRITICAL CVE: patch within 24 hours
- HIGH CVE: patch within 7 days
- MEDIUM CVE: patch within 30 days
- LOW CVE: patch at next sprint boundary

---

4. Dynamic Application Security Testing (DAST)

OWASP ZAP

Schedule: Monthly + before every major release

Scope (in-scope for ZAP):

- `https://staging.bilko.io` (staging environment only — NEVER production)
- All API endpoints under `/api/`
- Authentication flows
- File upload endpoints (if any)

Out of scope:

- SEF portal, FINA portal (external systems)
- Railway infrastructure
- Cloudflare WAF (managed by Cloudflare)

ZAP Configuration:

```
# zap-baseline.yaml
env:
  contexts:
    - name: Bilko API
      urls:
        - https://staging.bilko.io/api/
```

```
    authentication:
      method: script
      # ZAP script to authenticate and get JWT
  rules:
    - id: 10202  # Absence of Anti-CSRF tokens — note (cookies are httpOnly)
      threshold: LOW
    - id: 10096  # Timestamp Disclosure — ignore (timestamps are public)
      threshold: OFF
```

Required ZAP findings threshold (before release):

- CRITICAL / HIGH: 0 allowed
- MEDIUM: must be assessed — known acceptable risks documented
- LOW / INFORMATIONAL: document and prioritize

---

5. Penetration Testing

Frequency: Annual (or after significant architecture change) **Provider:** External certified pentest firm (OSCP/CREST certified)

Scope:

- Web application (app.bilko.io)
- API endpoints
- Authentication & session management
- Multi-tenant isolation (primary focus — org isolation must be tested)
- Business logic flaws (VAT calculation, invoice numbering)
- Third-party integrations (SEF API, HR-FISK)

Rules of engagement:

- Staging environment only — no production testing without explicit CEO approval
- No DoS / DDoS testing
- No social engineering of employees
- Penetration test agreement signed before engagement begins

Remediation SLAs (post-pentest findings):

Severity	Fix Deadline
CRITICAL	48 hours
HIGH	7 days

Severity	Fix Deadline
MEDIUM	30 days
LOW	Next quarter

---

6. Security Code Review

When required (mandatory pre-merge):

- Changes to authentication or authorization code
- Changes to encryption utilities (`encryptField`, `decryptField`)
- Changes to Prisma query patterns (potential org isolation bypass)
- New external API integrations (SEF, FINA, etc.)
- Changes to RBAC middleware or permission matrices

Who reviews: CTO or designated Senior Engineer with security background.

Checklist for security-sensitive PRs:

- ☐ No secrets or credentials in code or config
- ☐ All new Prisma queries include `organizationId` in WHERE clause
- ☐ New endpoints have RBAC decorator applied
- ☐ New user inputs validated with Zod schema
- ☐ L4 Restricted fields encrypted before write, decrypted after read
- ☐ LoggedAction entry created for all write operations
- ☐ Rate limiting applied to new auth-adjacent endpoints

---

7. CI/CD Security Gates

```
flowchart LR
    PR["Pull Request"] --> LINT["ESLint Security\nRules"]
    LINT -->|"PASS"| AUDIT["npm audit\n--audit-level=high"]
    AUDIT -->|"PASS"| TEST["Vitest\nSecurity Test Suite"]
    TEST -->|"PASS"| SECRETS["TruffleHog\nSecret Scan"]
    SECRETS -->|"PASS"| MERGE["Merge Allowed"]
    LINT -->|"FAIL"| BLOCK["PR Blocked"]
    AUDIT -->|"FAIL"| BLOCK
```

```
    TEST -->|"FAIL"| BLOCK
    SECRETS -->|"FAIL"| BLOCK
```

Non-negotiable gates (cannot be bypassed with `--no-verify` or `--force`):

1. ESLint security rules: zero `error` findings
2. npm audit: zero HIGH/CRITICAL CVEs
3. Vitest security tests: 100% pass — especially org isolation and RBAC tests
4. TypeScript strict: zero type errors

---

8. Vulnerability Disclosure

Process:

1. Security researchers may report vulnerabilities to security@bilko.io
2. Acknowledgment within 24 hours
3. Investigation and severity assessment within 5 business days
4. Remediation per SLA in Section 5
5. Responsible disclosure: researcher notified when fix is deployed

---

Approval

Role	Name	Signature	Date
Author	CTO / Security Engineer		2026-02-23
Reviewer (Engineering Lead)			
Reviewer (DPO)			
Approver	CEO		