Regulatory Compliance

Regulatory Compliance

Overview

Drop Srbija operates within the Serbian regulatory framework for payment services, data protection, and anti-money laundering. This document outlines the key legal requirements and compliance obligations.

NBS (Narodna Banka Srbije) — Payment Institution Licensing

Licensing Path

Year 1 (Recommended): Operate as **registered agent** under Article 24 of the Law on Payment Services through partnership with a licensed Serbian bank.

Year 2: Pursue **Payment Institution (PI) license** directly from NBS once market validation is proven.

Payment Institution License Requirements

If pursuing own PI license:

Minimum Capital Requirement: EUR 125,000 (or RSD equivalent)

Required Documents for NBS Authorization:

1. **Business Plan (3-year projection)**
   - Market analysis (Serbian remittance + domestic transfer market)
   - Revenue model (transaction fees, FX spreads)
   - Risk assessment (operational, financial, fraud, AML/CFT)
   - Financial projections (P&L, balance sheet, cash flow)

2. **AML/CFT Programme**
   - Customer due diligence procedures
   - Transaction monitoring rules (thresholds, alerts)
   - Sanctions screening process
   - Suspicious transaction reporting protocol
   - USPNFT eUprava integration for STR filing
3. **IT Security and Business Continuity**
   - System architecture diagram
   - Data protection measures (encryption, access control, audit logs)
   - Incident response plan
   - Disaster recovery and backup procedures
   - Penetration testing schedule
4. **Organizational Structure**
   - Org chart with key personnel
   - CVs and credentials of directors and compliance officers
   - Proof of fit-and-proper assessment (criminal record check, financial solvency)
   - Compliance Officer appointment (AML/CFT specialist)
   - Data Protection Officer (DPO) appointment
5. **Proof of Share Capital**
   - Bank statement showing EUR 125,000 deposited
   - Shareholder agreements
   - Proof of source of funds

Timeline: 9-14 months from application submission to license issuance (optimistic).

NBS Contact:

- Email: platne.institucije@nbs.rs
- Phone: +381 11 3027 100
- Address: Nemanjina 17, 11000 Belgrade, Serbia

Legal Reference: nbs-pisp-license-requirements.md

ZPNFTM (Zakon o spre?avanju pranja novca) — AML/CFT Framework

Law on Prevention of Money Laundering and Terrorist Financing

Official Gazette: 113/2017, 91/2019, 153/2020

Regulatory Authority: Administration for the Prevention of Money Laundering (APML)

Key Obligations

1. **Customer Due Diligence (CDD)**
   - Verify identity using government-issued ID (JMBG validation)
   - Collect name, address, date of birth, national ID number
   - Verify beneficial ownership (for legal entities)
   - Enhanced due diligence for high-risk customers (PEPs, high-value transactions)
2. **Transaction Monitoring**
   - Threshold: RSD 15,000 (~EUR 130) for identification requirement
   - High-value threshold: EUR 15,000 for enhanced monitoring
   - Pattern detection: Structuring, unusual activity, cross-border remittances
3. **Suspicious Transaction Reporting (STR)**
   - Report to APML via **USPNFT eUprava portal** (https://euprava.gov.rs)
   - No de minimis threshold — any suspicious activity must be reported
   - Prohibition on tipping off the customer
4. **Record Retention**
   - 5 years minimum for transaction data (Article 60)
   - 10 years for high-risk transactions
   - Must be readily accessible for APML audits
5. **Sanctions Screening**
   - Check all customers and transactions against:
     - **UN Consolidated List** (https://www.un.org/securitycouncil/sanctions/list)
     - **EU Restrictive Measures** (https://sanctionsmap.eu/)
     - **Serbian Government Sanctions** (Official Gazette)
   - **NOTE:** There is NO "NBS SDN list" — Serbia does not maintain a separate sanctions list. Use UN + EU + Serbian government sources only.
6. **PEP Screening**
   - Politically Exposed Persons (domestic and foreign)
   - Family members and close associates
   - Enhanced due diligence required

USPNFT eUprava Integration

Portal: https://euprava.gov.rs/usluge/uspnft
What it does: Electronic submission of Suspicious Transaction Reports (STRs) to APML

Drop Srbija Implementation:

- Compliance Officer has eUprava account with STR permissions
- STR submission within 3 business days of detection
- System generates draft STR from `aml_flags` table entries
- Manual review by Compliance Officer before submission

Legal Reference: framework-contract-payment-users-sr.md

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

Law on Personal Data Protection

Official Gazette: 87/2018

Regulatory Authority: Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti (Commissioner for Information of Public Importance and Personal Data Protection)

Contact:

- Email: office@poverenik.rs
- Phone: +381 11 3408 900
- Address: Bulevar kralja Aleksandra 15, 11000 Belgrade, Serbia

Key Principles

Serbia's ZZPL is modeled on GDPR but with some differences. Key provisions:

1. **Legal Bases for Processing (Article 12)**
   - **(a) Consent:** Marketing communications, optional features
   - **(b) Contract Performance:** Account creation, payment processing
   - **(c) Legal Obligation:** AML/CFT compliance, incident reporting to NBS
   - **(d) Vital Interests:** Fraud prevention
   - **(e) Public Interest:** Not applicable for Drop Srbija
   - **(f) Legitimate Interest:** Product improvements, analytics
2. **Data Categories Processed by Drop Srbija**
   - **Identity:** Name, JMBG (national ID), date of birth, address
   - **Contact:** Phone number, email
   - **Financial:** IBAN, transaction history
   - **Biometric (if KYC implemented):** Facial recognition data for identity verification
   - **Device:** IP address, device ID, app version
3. **Data Subject Rights**
   - **Right of Access (Article 23):** User can request copy of all personal data
   - **Right to Rectification (Article 24):** User can correct inaccurate data
   - **Right to Erasure (Article 25):** "Right to be forgotten" — must delete unless legal obligation to retain (AML 5-year retention overrides)

- **Right to Data Portability (Article 27):** Export data in machine-readable format (JSON)
- **Right to Object (Article 28):** User can object to processing based on legitimate interest

4. **Data Breach Notification**
   - **To Poverenik:** Within 72 hours of breach discovery (Article 54)
   - **To Users:** Without undue delay if high risk to rights and freedoms
   - **Breach Definition:** Unauthorized access, data loss, data exposure, ransomware, etc.
5. **Data Retention Policy**
   - **Active users:** Retain while account is active
   - **Inactive users:** After 2 years of inactivity, anonymize or delete (unless AML retention applies)
   - **AML data:** 5 years from transaction date (overrides erasure requests)
   - **Marketing consent:** Until withdrawn
6. **Cross-Border Data Transfers**
   - Drop Srbija infrastructure: AWS EU (Frankfurt or Stockholm region)
   - Serbia is an EU candidate country — adequacy decision expected during EU accession
   - Current status: Transfers to EU/EEA allowed under ZZPL Article 63 (adequate protection)

Data Protection Impact Assessment (DPIA)

Required for: Biometric KYC verification (facial recognition for JMBG validation)

Document: dpia-kyc-biometric.md

Key Findings:

- High risk: Biometric data is special category (Article 17)
- Mitigation: Encryption, access control, retention limits (delete after verification)
- Legal basis: Legal obligation (AML/CFT) + contract performance
- Approved by: ALAI Lexicon (awaiting Serbian DPO review)

Privacy Policy

Location: privacy-policy-sr.md

Publication Requirements:

- Must be in Serbian (official version)
- Published on Drop Srbija website before launch
- In-app display during onboarding (user must accept before account creation)

- Updated whenever processing activities change

Content Includes:

- Data controller: Drop Srbija d.o.o. (legal entity TBD)
- Legal bases for each processing activity
- Data categories and retention periods
- Third-party processors (AWS, SMS gateway)
- User rights and how to exercise them
- DPO contact details

Incident Reporting — NBS and Poverenik

Three-Track Notification System

Drop Srbija has three parallel incident notification obligations:

Track 1: NBS Initial Notification (Within 4 Hours)

Trigger: Significant operational or security incident affecting payment services

Examples:

- Service outage >2 hours
- Cyberattack or data breach
- Fraudulent transaction pattern
- NBS IPS integration failure
- Critical system failure

Contact: platne.institucije@nbs.rs, +381 11 3027 100

Format: Brief email alert with:

- Incident type and time of detection
- Preliminary impact assessment
- Immediate actions taken
- Estimated resolution time

Track 2: NBS Detailed Report (Within 72 Hours)

Follow-up to Track 1 with comprehensive analysis:

Required Content:

- Root cause analysis
- Full impact assessment (customers affected, transaction volume, financial loss)
- Timeline of events
- Preventive measures implemented
- Lessons learned

Format: PDF document, 5-15 pages, Serbian language

Submission: Email to platne.institucije@nbs.rs

Track 3: Poverenik Data Breach Notification (Within 72 Hours)

Trigger: Personal data breach (unauthorized access, data exposure, data loss)

Examples:

- Database leak
- Phishing attack exposing customer data
- Employee unauthorized access
- Ransomware encryption of customer records

Contact: office@poverenik.rs, +381 11 3408 900

Format: Breach notification form (available on Poverenik website)

Required Content:

- Nature of breach (type of data, number of individuals affected)
- Likely consequences
- Measures taken to mitigate
- DPO contact details

IMPORTANT: This is a separate notification from NBS reporting. Personal data breaches must be reported to BOTH NBS (if affecting payment services) AND Poverenik (for data protection compliance).

User Notification

Trigger: Data breach likely to result in high risk to user rights and freedoms

Timeline: Without undue delay (typically within 72 hours)

Method: SMS + in-app notification + email

Template: incident-notification-procedure.md contains user notification templates in Serbian.

Serbian Bank Partnership

Drop Srbija Year 1 strategy relies on partnership with a licensed Serbian bank to access NBS IPS as a registered agent.

Legal Framework: Article 24 (Agent Registration)

Under the Law on Payment Services, payment institutions and banks can appoint **registered agents** to provide payment services on their behalf.

Requirements:

- Agent must be registered with NBS
- Principal (bank) remains responsible for agent's actions
- Written agent agreement required
- Agent must comply with all AML/CFT obligations

Bank Partnership Pitch

Target Banks: Raiffeisen Banka, Erste Bank, Banca Intesa, OTP Banka, Mobi Banka (digital-first)

Value Proposition:

- Drop brings new digital-native customers to the bank
- Increased IPS transaction volume
- Revenue share on transaction fees
- Co-branded offering (optional)

What Drop Needs:

- IPS gateway API access
- Registered agent status (Article 24)
- Technical integration support
- Bank account for settlement

Document: serbian-bank-partnership-pitch.md

Timeline: 6-7 months from first contact to launch (optimistic)

Sanctions Sources (CORRECTED)

Drop Srbija screens against three sources:

1. **UN Consolidated List**
   - URL: https://www.un.org/securitycouncil/sanctions/list
   - Format: XML/PDF download
   - Update frequency: Weekly
2. **EU Restrictive Measures (Sanctions Map)**
   - URL: https://sanctionsmap.eu/
   - Format: JSON API available
   - Update frequency: Daily
3. **Serbian Government Sanctions**
   - Source: Official Gazette of the Republic of Serbia
   - Implementation: Serbia adopts UN sanctions, occasionally imposes additional measures
   - No centralized API — manual monitoring required

CRITICAL CORRECTION: There is NO "NBS SDN list." NBS does not maintain a separate sanctions list. Earlier references to "NBS SDN" were an error. Use only the three sources above.

Compliance Roles

Drop Srbija must appoint the following officers before launch:

Role	Responsibility	Qualifications
Data Protection Officer (DPO)	ZZPL compliance, data subject requests, breach notification	Legal/IT background, ZZPL expertise
AML/CFT Compliance Officer	Transaction monitoring, STR filing, sanctions screening	ACAMS certification or equivalent, Serbian language
Risk Officer	Operational and financial risk management	Can be CTO initially, fintech risk experience

Hiring Status: TBD — awaiting Drop Srbija d.o.o. incorporation

---

Legal Document Index

All legal and compliance documents are located in `/comms/decisions/`:

- nbs-pisp-license-requirements.md — NBS PI license application guide
- serbian-bank-partnership-pitch.md — Bank partnership proposal template
- privacy-policy-sr.md — ZZPL-compliant privacy policy (Serbian)
- privacy-policy-drop-srbija-draft.md — Privacy policy (English draft)
- incident-notification-procedure.md — Three-track incident reporting protocol
- dpia-kyc-biometric.md — DPIA for biometric KYC
- framework-contract-payment-users-sr.md — Framework contract for payment service users
- recommendation-year1-vs-year2.md — Finverge analysis: Agent model vs PI license
- serbian-banks-api-landscape.md — Serbian banking API research
- nbs-pi-license-application-package.md — Complete NBS application package guide

---

DISCLAIMER:

All documents are DRAFT status and require Serbian legal counsel review before use. Drop Srbija must engage a Serbian law firm specializing in fintech/payment services for:

1. Validation of all legal and regulatory statements
2. Review and finalization of all documents
3. Entity structure and licensing strategy advice
4. Drafting final agreements and regulatory submissions

Budget Estimate: EUR 5,000-10,000 for initial legal review.

Last Updated: 2026-04-16
Next Review: After Serbian legal counsel engagement

Revision #2
Created 2026-04-16 22:35:14 UTC by John
Updated 2026-05-31 20:06:05 UTC by John