POLITIKA PRIVATNOSTI / PRIVACY POLICY (SR/EN)

Datum / Date: 23. novembar 2025. / 23 November 2025
Verzija / Version: 1.5

RS SRPSKA VERZIJA

Rukovalac podacima

Sindikat NCR Atleos – Beograd
Adresa: Španskih Boraca 75, 11070 Novi Beograd, Srbija
Kontakt: office@sindikatncr.com | +381 66 138 034

---

1. Ova Politika i ko smo „mi"

Ova Politika objašnjava kako Sindikat NCR Atleos – Beograd („Sindikat", „mi") prikuplja i obrađuje lične podatke kada koristite naš sajt (sindikatncr.com) i povezane usluge (e-prijava, kontakt forma, administracija). Mi smo rukovalac (kontrolor) u smislu Zakona o zaštiti podataka o ličnosti ("Sl. glasnik RS", br. 87/2018) i GDPR-a.

---

2. Načela obrade

Obrada podataka o ličnosti vrši se u skladu sa sledećim principima:

- **Zakonitost, poštenost, transparentnost**
- **Ograničenje svrhe**
- **Minimizacija podataka**
- **Tačnost**
- **Ograničenje čuvanja**
- **Integritet i poverljivost**

---

3. Tokovi obrade i pravni osnovi

3.1. Podaci o sindikalnom članstvu

Podaci koje prikupljamo:

- Ime i prezime (obavezno)
- Email adresa (obavezno)
- Quicklook ID – QLID (obavezno)
- Grad (obavezno)
- Organizacija/jedinica (opciono)
- Metapodaci o podnošenju (ID zahteva, datum/vreme, IP u obliku heša)

Svrha: Evidencija članstva, interna komunikacija sa članovima, verifikacija uslova za članstvo i organizaciona podrška sindikalnim aktivnostima.

Pravni osnov:

- Član 12. stav 1. tačka 2) Zakona o zaštiti podataka o ličnosti (izvršenje predugovornih/ugovornih radnji u vezi sa članstvom)
- Član 17. stav 2. tačka 4) i tačka 2) Zakona (obrada od strane sindikata u okviru zakonitih aktivnosti sa odgovarajućim garancijama)
- Ekvivalentno: Art. 6(1)(b) i Art. 9(2)(d) GDPR-a

Privatnost do reprezentativnosti:
Identitet članova i povezivi podaci dostupni su isključivo predsedniku i ovlašćenim licima sindikata uz stroge tehničke i organizacione mere (RBAC/RLS, evidencije pristupa, enkripcija). Podaci se obrađuju samo u meri neophodnoj za vođenje evidencije i zaštitu prava članova. Po sticanju reprezentativnosti, podaci se mogu koristiti za zakonite aktivnosti kolektivnog pregovaranja u skladu sa zakonom.

Dobrovoljna vidljivost:
Član može izabrati status „vidljiv" radi učešća u aktivnom radu sindikata; ta izborna promena važi za ubuduće i može biti opozvana.

3.2. Kontakt forma

Podaci: Ime (opciono), email (opciono), poruka (obavezno), IP heš i vreme slanja.

Svrha: Odgovor na upit.

Pravni osnov: Član 12. stav 1. tačka 6) Zakona (legitimni interesi); ekvivalentno Art. 6(1)(f) GDPR-a.

3.3. Administracija (NextAuth)

Podaci: Minimalni OAuth profil (npr. email), sesija/JWT, tehnički kolačići.

Svrha: Upravljanje pristupom administracijskom panelu.

Pravni osnov: Član 12. stav 1. tačka 6) Zakona (legitimni interesi).

3.4. Analitika (Plausible – cookieless)

Podaci: Agregatne metrike bez identifikacije posetilaca.

Svrha: Razumevanje korišćenja sajta.

Pravni osnov: Član 12. stav 1. tačka 6) Zakona (legitimni interesi).

3.5. Zaštita od zloupotrebe (reCAPTCHA Enterprise / Cloudflare Turnstile)

Podaci: Tehnički signali za prepoznavanje botova.

Svrha: Zaštita od automatizovanih napada.

Pravni osnov: Član 12. stav 1. tačka 6) Zakona (legitimni interesi).

3.6. Transakcioni email (Resend i/ili Hostinger)

Podaci: Adresa primaoca, tehnički metapodaci, sadržaj poruke u meri neophodnoj za isporuku.

Svrha: Slanje transakcionalnih poruka.

Pravni osnovi:

- Član 12. stav 1. tačka 2) Zakona (izvršenje ugovora)
- Član 12. stav 1. tačka 6) Zakona (legitimni interesi)
- Član 17. stav 2. tačka 2) ili 4) Zakona (gde primenljivo)

---

4. Metode verifikacije

Nudimo više načina za prijavljivanje, sa različitim nivoima privatnosti:

1. ✅ **Lična prijava kod predstavnika** – najbezbednije, bez digitalnog traga
2. ✅ **Upload dokaza zaposlenja** – dokument se odmah briše nakon verifikacije
3. ⚠️ **Interni chat sistem** – može biti vidljivo IT službi
4. ⚠️ **Službeni email** – poslodavac može videti komunikaciju

⚠️ **Upozorenje**

Ne preporučujemo korišćenje poslovnih sistema (email, chat, računara) za sindikalne aktivnosti jer poslodavac može videti vašu komunikaciju. Koristite na sopstveni rizik.

---

5. Quicklook ID (QLID)

Svrha: Isključivo provera ispunjenosti uslova za članstvo (zaposlenje u NCR ATM doo).

Minimizacija: QLID se ne koristi za profilisanje, marketing ili bilo koju drugu svrhu i ne deli se sa poslodavcem.

Napomena: QLID je javno dostupan na Microsoft Teams-u, što omogućava bezbedno čuvanje u bazi bez dodatne enkripcije.

---

6. Mesečna provera aktivnog članstva

Svaki mesec poredimo listu aktivnih sindikalnih članova sa listom zaposlenih u firmi koristeći Quicklook ID (QLID). Ako član više nije zaposlen, automatski se označava kao neaktivan.

---

7. Primaoci (obrađivači) i prenosi

Koristimo sledeće obrađivače sa potpisanim ugovorima o zaštiti podataka (DPA; SCC/TIA pri prenosu van EEA):

Supabase

- **Lokacija:** EU
- **Upotreba:** Baza podataka, autentifikacija, serverless funkcije
- **Podaci:** Zapisi o članstvu, minimalni podaci o nalogu, logovi/metapodaci
- **Transfer:** SCC + TIA ako van EEA

Vercel

- **Lokacija:** EU
- **Upotreba:** Hosting, CDN, edge servisi
- **Podaci:** Serverski logovi/metapodaci, tragovi grešaka (bez PII tereta)
- **Transfer:** SCC + TIA ako van EEA

Resend

- **Lokacija:** EU
- **Upotreba:** Email servis (transakcione poruke)
- **Podaci:** Email primaoca, metapodaci dostave, sadržaj poruke (minimalno)
- **Transfer:** SCC + TIA

Plausible

- **Lokacija:** EU
- **Upotreba:** Cookieless analitika
- **Podaci:** Agregatne metrike korišćenja (bez identifikatora)
- **Transfer:** EU-based; bez transfera van EEA

Hostinger

- **Lokacija:** EU
- **Upotreba:** Email i hosting servisi
- **Podaci:** Email adresa, metapodaci poruke, telo poruke ako je rutirana
- **Transfer:** SCC + TIA ako van EEA

Google reCAPTCHA Enterprise

- **Upotreba:** Zaštita od zloupotrebe/botova
- **Podaci:** Signali uređaja/korišćenja, IP, zaglavlja (prema Google politici)
- **Transfer:** SCC/DPF + TIA

Cloudflare Turnstile (opciono/alternativa)

- **Upotreba:** Zaštita od zloupotrebe/botova
- **Podaci:** Signali izazova, IP, zaglavlja (prema Cloudflare politici)
- **Transfer:** SCC + TIA

Discord Lokacija: SAD (Discord Inc., San Francisco, CA)

- **Upotreba:** Interne notifikacije administratorima o novim prijavama članova
- **Podaci:** Ime i prezime, email adresa, Quicklook ID, grad, odeljenje, tim, status anonimnosti, datum prijave
- **Transfer:** Standardni ugovorni uslovi (SCC) prema GDPR-u Napomena: Discord webhook koristi se samo za slanje notifikacija administratorima sindikata. Podaci nisu javno dostupni i vidljivi su samo ovlašćenim licima sindikata.

---

8. Bezbednosne mere (TOMs)

Primenjuju se sledeće tehničke, organizacione i kadrovske mere (u skladu sa članom 50. i 51. Zakona):

- Multifaktorska autentifikacija (MFA/2FA)
- Kontrola pristupa na osnovu uloga (RBAC – least-privilege principle)
- Kontrola pristupa na nivou redova (RLS)
- Enkripcija u prenosu i mirovanju

- Rotacija tajnih ključeva
- Auditovanje pristupa
- Rezervne kopije + periodični testovi obnavljanja
- Plan odgovora na incidente

---

9. Rokovi čuvanja

Podaci se čuvaju samo onoliko koliko je neophodno za ostvarivanje svrhe obrade (u skladu sa članom 5. stav 1. tačka 5) Zakona):

- **Članstvo:** Trajanje članstva + 3 godine
- **Kontakt upiti:** Do 12 meseci
- **Logovi:** 30–90 dana
- **Admin sesije:** Prema postavkama

Napomena: Mesečne provere statusa se ne čuvaju kao istorija, već se koriste samo za ažuriranje statusa.

Po isteku rokova – brisanje ili anonimizacija podataka.

---

10. Prava lica na koje se podaci odnose

Imate sledeća prava (u skladu sa članom 26. do 39. Zakona):

- **Pristup** vašim podacima (Član 26.)
- **Ispravka** netačnih podataka (Član 29.)
- **Brisanje** ("pravo na zaborav") (Član 30.)
- **Ograničavanje obrade** (Član 31.)
- **Prenosivost podataka** u strukturisanom, mašinski čitljivom formatu (Član 36.)
- **Prigovor** na obradu zasnovanu na legitimnim interesima (Član 37.)

- **Povlačenje saglasnosti** (ako je primenljivo) – bez uticaja na zakonitost obrade do povlačenja

Zahtevi se podnose na: office@sindikatncr.com

Odgovorna vremenska linija: Bez odlaganja, najkasnije u roku od 30 dana od prijema zahteva (može biti produženo za 60 dana ako je kompleksno).

---

11. Nadzorni organ

Ako smatrate da je vaše pravo na zaštitu podataka narušeno, možete podneti pritužbu:

Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti
Email: office@poverenik.rs
Telefon: +381 11 3408 900

---

12. Kolačići i slične tehnologije

Preferiramo cookieless analitiku (Plausible) i ne koristimo marketinške kolačiće. Tehnički kolačići za sesiju i zaštitu od zloupotrebe mogu biti neophodni, u skladu sa članom 128a Zakona o elektronskim komunikacijama ("Sl. glasnik RS", br. 44/2010, 60/2013, 62/2014, 95/2018).

---

13. Deca

Usluge nisu namenjene licima mlađim od 16 godina. Ako sumnjamo da je lice mlađe od 16 godina pružilo podatke, obrisaćemo te podatke bez odlaganja, u skladu sa članom 13. stav 3. Zakona.

---

14. Povrede bezbednosti podataka

U slučaju povrede bezbednosti podataka o ličnosti, lica će biti obaveštena bez odlaganja, u skladu sa članom 52. i 53. Zakona:

- Priroda povrede

- Verovatni uticaj
- Preporučene mere
- Poverenik će biti obavešten prema zahtevima Zakona

---

15. Izmene Politike

Najnovija verzija politike dostupna je na sindikatncr.com/politika-privatnosti. O bitnim izmenama obaveštavamo članove na odgovarajući način, u skladu sa članom 24. Zakona.

---

16. Kontakt

Sindikat NCR Atleos – Beograd
Španskih Boraca 75, 11070 Novi Beograd, Srbija
office@sindikatncr.com | +381 66 138 034

Poslednja izmena: 15. novembar 2025.

GB ENGLISH VERSION

Data Controller

NCR Atleos – Belgrade Employees' Union
Address: Španskih Boraca 75, 11070 New Belgrade, Serbia
Contact: office@sindikatncr.com | +381 66 138 034

---

1. This Policy and Who We Are

This Policy explains how NCR Atleos – Belgrade Employees' Union ("Union", "we") collects and processes personal data when you use our website (sindikatncr.com) and related services (e-application, contact form, administration). We act as the data controller under the Personal Data Protection Act ("Official Gazette RS", No. 87/2018) and GDPR.

---

2. Processing Principles

Personal data processing is carried out in accordance with the following principles:

- **Lawfulness, fairness, transparency**
- **Purpose limitation**
- **Data minimization**
- **Accuracy**
- **Storage limitation**
- **Integrity and confidentiality**

---

3. Processing Activities and Legal Bases

3.1. Union Membership Data

Data we collect:

- Full name (required)
- Email address (required)
- Quicklook ID – QLID (required)

- City (required)
- Organization/unit (optional)
- Submission metadata (request ID, date/time, IP in hashed form)

Purpose: Membership records, internal member communication, membership eligibility verification, and organizational support for union activities.

Legal basis:

- Article 12, paragraph 1, item 2) of the Personal Data Protection Act (performance of pre-contractual/contractual actions related to membership)
- Article 17, paragraph 2, items 4) and 2) of the Act (processing by a trade union in the course of its legitimate activities with appropriate safeguards)
- Equivalent: Art. 6(1)(b) and Art. 9(2)(d) GDPR

Privacy until representativeness:
Member identities and linkable data are accessible only to the President and authorized union officials under strict technical and organizational measures (RBAC/RLS, access logs, encryption). Data is processed only to the extent necessary for maintaining records and protecting members' rights. Upon achieving representativeness, data may be used for lawful collective bargaining activities in accordance with the law.

Voluntary visibility:
A member may choose "visible" status for active participation in union work; this optional change applies going forward and can be revoked.

3.2. Contact Form

Data: Name (optional), email (optional), message (required), IP hash and submission time.

Purpose: Respond to inquiry.

Legal basis: Article 12, paragraph 1, item 6) of the Act (legitimate interests); equivalent to Art. 6(1)(f) GDPR.

3.3. Administration (NextAuth)

Data: Minimal OAuth profile (e.g., email), session/JWT, technical cookies.

Purpose: Managing access to administrative panel.

Legal basis: Article 12, paragraph 1, item 6) of the Act (legitimate interests).

3.4. Analytics (Plausible – cookieless)

Data: Aggregate metrics without visitor identification.

Purpose: Understanding website usage.

Legal basis: Article 12, paragraph 1, item 6) of the Act (legitimate interests).

3.5. Anti-abuse Protection (reCAPTCHA Enterprise / Cloudflare Turnstile)

Data: Technical signals for bot detection.

Purpose: Protection against automated attacks.

Legal basis: Article 12, paragraph 1, item 6) of the Act (legitimate interests).

3.6. Transactional Email (Resend and/or Hostinger)

Data: Recipient address, technical metadata, message content to the extent necessary for delivery.

Purpose: Sending transactional messages.

Legal bases:

- Article 12, paragraph 1, item 2) of the Act (contract performance)
- Article 12, paragraph 1, item 6) of the Act (legitimate interests)
- Article 17, paragraph 2, items 2) or 4) of the Act (where applicable)

---

4. Verification Methods

We offer multiple application methods with different privacy levels:

1. ✅ **In-person application with representative** – most secure, no digital trace
2. ✅ **Upload proof of employment** – document deleted immediately after verification
3. ⚠️ **Internal chat system** – may be visible to IT department
4. ⚠️ **Work email** – employer may see communication

⚠️ **Warning**

We do not recommend using corporate systems (email, chat, computers) for union activities as your employer may see your communication. Use at your own risk.

---

5. Quicklook ID (QLID)

Purpose: Solely to verify membership eligibility (employment at NCR ATM doo).

Minimization: QLID is not used for profiling, marketing, or any other purpose and is not shared with the employer.

Note: QLID is publicly available on Microsoft Teams, which enables secure database storage without additional encryption.

---

6. Monthly Active Membership Verification

Every month we compare the list of active union members with the company's employee list using Quicklook ID (QLID). If a member is no longer employed, they are automatically marked as inactive.

---

7. Recipients (Processors) and Transfers

We use the following processors with signed Data Processing Agreements (DPA; SCC/TIA for transfers outside EEA):

Supabase

- **Location:** EU
- **Use:** Database, authentication, serverless functions
- **Data:** Membership records, minimal account data, logs/metadata
- **Transfer:** SCC + TIA if outside EEA

Vercel

- **Location:** EU
- **Use:** Hosting, CDN, edge services
- **Data:** Server logs/metadata, error traces (no payload PII)

- **Transfer:** SCC + TIA if outside EEA

Resend

- **Location:** EU
- **Use:** Email service (transactional messages)
- **Data:** Recipient email, delivery metadata, message content (minimal)
- **Transfer:** SCC + TIA

Plausible

- **Location:** EU
- **Use:** Cookieless analytics
- **Data:** Aggregate usage metrics (no identifiers)
- **Transfer:** EU-based; no transfer outside EEA

Hostinger

- **Location:** EU
- **Use:** Email and hosting services
- **Data:** Email address, message metadata, message body if routed
- **Transfer:** SCC + TIA if outside EEA

Google reCAPTCHA Enterprise

- **Use:** Anti-abuse/bot protection
- **Data:** Device/usage signals, IP, headers (per Google policy)
- **Transfer:** SCC/DPF + TIA

Cloudflare Turnstile (optional/alternative)

- **Use:** Anti-abuse/bot protection
- **Data:** Challenge signals, IP, headers (per Cloudflare policy)
- **Transfer:** SCC + TIA

Discord USA (Discord Inc., San Francisco, CA)

- **Use:** Internal notifications to administrators about new member applications
- **Data:** Full name, email address, Quicklook ID, city, division, team, anonymity status, application date
- **Transfer:** Standard Contractual Clauses (SCC) under GDPR Note: Discord webhook is used only for sending notifications to union administrators. Data is not publicly available and visible only to authorized union officials.

---

8. Security Measures (TOMs)

The following technical, organizational, and personnel measures are implemented (in accordance with Articles 50 and 51 of the Act):

- Multi-factor authentication (MFA/2FA)
- Role-based access control (RBAC – least-privilege principle)
- Row-level security (RLS)
- Encryption in transit and at rest
- Secret key rotation
- Access auditing
- Backups + periodic restore testing
- Incident response plan

---

9. Retention Periods

Data is retained only as long as necessary to achieve the processing purpose (in accordance with Article 5, paragraph 1, item 5) of the Act):

- **Membership:** Duration of membership + 3 years
- **Contact inquiries:** Up to 12 months
- **Logs:** 30–90 days
- **Admin sessions:** According to settings

Note: Monthly status checks are not stored as history but are used only for status updates.

Upon expiry – data deletion or anonymization.

---

10. Data Subject Rights

You have the following rights (in accordance with Articles 26 to 39 of the Act):

- **Access** to your data (Article 26)
- **Rectification** of inaccurate data (Article 29)
- **Erasure** ("right to be forgotten") (Article 30)
- **Restriction** of processing (Article 31)
- **Data portability** in structured, machine-readable format (Article 36)
- **Objection** to processing based on legitimate interests (Article 37)
- **Withdrawal of consent** (if applicable) – without affecting the lawfulness of processing before withdrawal

Requests should be submitted to: office@sindikatncr.com

Response timeline: Without delay, at the latest within 30 days of receiving the request (may be extended by 60 days if complex).

---

11. Supervisory Authority

If you believe your data protection rights have been violated, you may file a complaint with:

Commissioner for Information of Public Importance and Personal Data Protection
Email: office@poverenik.rs
Phone: +381 11 3408 900

---

12. Cookies and Similar Technologies

We prefer cookieless analytics (Plausible) and do not use marketing cookies. Technical cookies for session and anti-abuse protection may be necessary, in accordance with Article 128a of the Electronic Communications Act ("Official Gazette RS", No. 44/2010, 60/2013, 62/2014, 95/2018).

---

13. Children

Services are not intended for persons under 16 years of age. If we suspect that a person under 16 has provided data, we will delete such data without delay, in accordance with Article 13, paragraph 3 of the Act.

---

14. Personal Data Security Breaches

In case of a personal data security breach, individuals will be notified without delay, in accordance with Articles 52 and 53 of the Act:

- Nature of the breach
- Probable impact
- Recommended measures
- The Commissioner will be notified according to Act requirements

---

15. Policy Changes

The latest version of the policy is available at sindikatncr.com/politika-privatnosti. We notify members of material changes appropriately, in accordance with Article 24 of the Act.

---

16. Contact

Employees' Union NCR Atleos – Belgrade
Španskih Boraca 75, 11070 New Belgrade, Serbia
office@sindikatncr.com | +381 66 138 034