Master Privacy Policy

Centrul de Calcul SA

Qualified Trust Service Provider (QTSP)

Applicant — European Digital Identity (EUDI) Wallet Accreditation

Effective Date: 20 April 2026

Version: 1.1

Document Language: English (the Romanian version is published separately)

Preamble

This Master Privacy Policy (the "Policy") describes how Centrul de Calcul SA ("Centrul de Calcul", "we", "us", or "our") collects, uses, stores, and protects your personal data across its mobile applications, web-based Software-as-a-Service (SaaS) platforms, desktop software, and its European Digital Identity (EUDI) Wallet and Qualified Trust Services.

We designed this Policy to fulfil the transparency requirements of Article 12 of the General Data Protection Regulation (GDPR). It is written in clear and plain language and is organised as a modular document: a universal baseline that applies to every product, followed by application-specific chapters that address the unique characteristics of each product family.

Centrul de Calcul SA was established in Romania in 1976 and operates as a Qualified Trust Service Provider under Regulation (EU) No 910/2014 (eIDAS). We are currently pursuing accreditation for EUDI Wallet services under Regulation (EU) 2024/1183 (eIDAS 2.0). Our processing of personal data is further governed by Romanian Law No. 190/2018, Romanian Law No. 506/2004, and Directive (EU) 2022/2555 (NIS2), alongside the NIST Cybersecurity Framework.

1. Introduction, Scope, and Definitions

1.1 The Data Controller

The Data Controller for the personal data processed in connection with the services described in this Policy is:

- **Legal Name:** Centrul de Calcul SA
- **Registered Office:** Targu Jiu, Gorj, Romania
- **Primary Contact:** sediu@centruldecalcul.ro
- **Website:** https://centruldecalcul.ro
- **Website:** https://certdigital.ro

1.2 Scope of the Policy

This Policy applies to every interaction you have with Centrul de Calcul SA through the following categories of products and services:

- Mobile applications distributed through the Apple App Store and the Google Play Store;
- Web-based Software-as-a-Service (SaaS) platforms delivered from centruldecalcul.ro and associated subdomains;

- Desktop software and on-premises client applications installed on your workstation or within your organisation's intranet;
- The European Digital Identity (EUDI) Wallet and the associated Qualified Trust Services (qualified certificates, qualified electronic signatures and seals, qualified timestamps, qualified validation and preservation services, and remote identity proofing).

1.3 Definitions

To make this Policy intelligible to every reader, the following key terms have the meaning given below:

- **Personal Data —** Any information relating to an identified or identifiable natural person.
- **Data Controller —** The entity that determines the purposes and means of processing.
- **Data Processor —** A third party that processes personal data on behalf of and strictly on the instructions of the Controller.
- **Qualified Trust Service Provider (QTSP) —** An entity accredited under eIDAS to provide qualified electronic trust services.
- **Relying Party —** Any public or private entity that requests, receives, or validates information from your EUDI Wallet.
- **EUDI Wallet —** The European Digital Identity Wallet defined by Regulation (EU) 2024/1183.
- **CNP —** The Romanian personal numerical code, a national identifier assigned to each citizen.
- **ANSPDCP —** The Romanian National Supervisory Authority for Personal Data Processing.

2. Oversight: The Data Protection Officer (DPO)

Because the services provided by Centrul de Calcul SA involve the large-scale processing of national identifiers and other sensitive data, we have appointed a Data Protection Officer (DPO) as required by Article 37 of the GDPR and by Article 10 of Romanian Law No. 190/2018.

2.1 Contact Details of the DPO

- **Email:** dpo@centruldecalcul.ro
- **Postal address:** Data Protection Officer, Centrul de Calcul SA, Targu Jiu, Gorj, Romania

You may contact the DPO directly and confidentially on any matter related to the processing of your personal data or the exercise of your rights under the GDPR.

2.2 DPO Oversight of the Romanian Personal Numerical Code (CNP)

In our capacity as a QTSP we are required to collect and process the Romanian personal numerical code (CNP), identity card series and numbers, and passport numbers in order to issue qualified certificates and operate the EUDI Wallet. Article 4 of Law No. 190/2018 imposes strict conditions on the processing of such national identifiers.

Where we rely on the legitimate interest of the Controller under Article 6(1)(f) of the GDPR to process the CNP, Law No. 190/2018 triggers the mandatory appointment of a DPO and the implementation of dedicated safeguards. The DPO therefore exercises specific, documented oversight over:

- The collection, storage, and use of the CNP and of the national identification numbers accompanying it;
- Access control and audit logging of any internal query involving these identifiers;
- The duration of storage and the secure erasure of these identifiers at the end of their retention period;
- The review of any proposed new processing activity that would involve the CNP, prior to its deployment.

Through this dedicated oversight we ensure that highly sensitive national identifiers are subject to a stricter internal regulatory supervision than any other category of personal data.

3. Universal Principles of Data Processing

Every engineering team, operations team, and third party acting on our behalf is bound by the following GDPR core principles, which are embedded in the design of every product we offer:

- **Lawfulness, Fairness, and Transparency —** We only process personal data where we have an identified lawful basis and we always disclose how we use it.
- **Purpose Limitation —** We collect personal data for specified, explicit, and legitimate purposes, and we do not further process it in ways incompatible with those purposes.
- **Data Minimisation —** We only collect what is strictly necessary to deliver the requested service, with special attention to EUDI Wallet selective disclosure.
- **Accuracy —** We take every reasonable step to keep personal data accurate and up to date and to give you the means to correct it.
- **Storage Limitation —** We retain personal data only for as long as necessary for the purposes for which it is processed, subject to the overriding legal retention periods applicable to QTSP activities.
- **Integrity and Confidentiality —** We protect personal data through state-of-the-art cryptography, strict access control, multi-factor authentication, monitored logging, and continuous threat detection.

- **Accountability —** We document and continuously audit our compliance with each of the above principles and with every applicable legal obligation.

4. Categories of Data Collected and Lawful Bases for Processing

The following matrix maps each category of personal data we collect to its representative elements, its processing purpose, and its lawful basis under the GDPR. Where special categories of data are involved (for example biometric or health data), we rely on Article 9(2)(a) of the GDPR and on Article 3 of Law No. 190/2018, both of which require your explicit, unambiguous consent or an express legal provision combined with appropriate safeguards.

Data Category	Representative Data Elements	Purpose of Processing	Lawful Basis (GDPR)
Account & Core Identity	Name, Email Address, CNP, Phone Number	Service provisioning, account management, QTSP identity verification	Art. 6(1)(b) Contract; Art. 6(1)(c) Legal Obligation; Art. 6(1)(f) Legitimate Interest
Financial & Billing Data	Billing address, payment history, transaction records	Subscription management, invoicing, financial compliance	Art. 6(1)(b) Contract; Art. 6(1)(c) Legal Obligation
Technical & Device Data	IP Address, Operating System, Unique Device Identifiers	Security monitoring, fraud prevention, software stability analytics	Art. 6(1)(f) Legitimate Interest
Biometric Data	Facial vectors generated during onboarding	Remote identity proofing for the issuance of Qualified Trust Services	Art. 9(2)(a) Explicit Consent
Special Category Data	Health data, union membership (if applicable to specific apps)	Provisioning of specialized software modules	Art. 9(2)(a) Explicit Consent or specific legal derogations

4.1 Legitimate Interest and Balancing Test

Wherever we rely on Article 6(1)(f) of the GDPR — for example to deliver software telemetry, run security log analytics, or prevent fraud — we have carried out and documented a balancing test demonstrating that the commercial interests of Centrul de Calcul SA do not override your

fundamental rights and freedoms. You may request a summary of this assessment by writing to the DPO.

4.2 Special Categories of Data and Explicit Consent

The biometric processing that enables remote video identity proofing for the issuance of qualified certificates, and any special-category processing that may take place in specialised applications, are always based on your explicit consent. This consent is separately requested, granularly described, and freely revocable.

5. Trust Services and eIDAS 2.0 Specific Provisions

The EUDI Wallet provided by Centrul de Calcul SA is engineered under Regulation (EU) 2024/1183 (eIDAS 2.0) and operationalises the GDPR principles of Data Protection by Design and by Default directly inside its cryptographic architecture.

5.1 Sole User Control and Local Storage

You retain sole and exclusive control over your European Digital Identity Wallet. Your Personal Identification Data (PID) and your Electronic Attestations of Attributes (EAAs) — such as a mobile driving licence, educational credentials, or financial attestations — are stored locally on the secure hardware of your device (for example the secure enclave of your smartphone). They are not stored on central servers operated by Centrul de Calcul SA or by the Romanian state.

5.2 Selective Disclosure and Zero-Knowledge Proofs (ZKPs)

The Wallet is equipped with advanced privacy-enhancing technologies — Selective Disclosure and Zero-Knowledge Proofs (ZKPs) — that allow you to share only the specific, granular attributes requested by a Relying Party, without disclosing the entirety of a credential.

For example, you can cryptographically prove that you are over 18 years of age without revealing your exact date of birth, your name, or your address. This minimises the attack surface for identity fraud and enforces the GDPR data minimisation principle at the protocol level.

5.3 Unlinkability and Unobservability

Pursuant to Article 5a of Regulation (EU) 2024/1183, the Wallet guarantees the properties of unlinkability and unobservability. We, acting as the Wallet provider, are technically and procedurally incapable of tracking, observing, or profiling your interactions or transactions.

The architecture ensures that neither the Wallet provider nor the original credential issuer receives any notification or telemetry when you present a document to a Relying Party. This cryptographic unobservability prevents the compilation of behavioural profiles and safeguards you against surveillance.

5.4 Separation of QTSP Datasets

Under Article 45h of eIDAS 2.0, identity data generated through our Qualified Trust Services is logically and organisationally separated from any other dataset produced by any other commercial service offered by Centrul de Calcul SA. We strictly forbid the combination, cross-referencing, or pooling of highly sensitive trust service identity data with marketing data, telemetry, or any other commercial dataset.

5.5 The Built-in Privacy Dashboard

The Wallet includes a comprehensive, user-facing Privacy Dashboard that serves as your single point of control. From the Dashboard you can:

- Review a complete, up-to-date log of every attribute you have disclosed and to which Relying Party;
- Review the registry of Relying Parties you have interacted with and revoke future access;
- Submit a Data Deletion Request directly to a Relying Party (specification EC TS07 v1.0) under Article 17 of the GDPR;
- Submit a Complaint about an unlawful or suspicious request directly to the ANSPDCP (specification EC TS08 v0.95) from within the application;
- Verify the cryptographic identity and legal status of any Relying Party through the "Trust Mark UI view".

Before any transmission of data, the Wallet evaluates the machine-readable privacy policy — often expressed in the Digital Credentials Query Language (DCQL) — embedded by the Relying Party, so that you can approve or deny the request with full awareness of its purpose.

5.6 Overriding QTSP Retention Mandates

While the GDPR emphasises storage limitation, eIDAS and Romanian national law impose specific, extended retention periods on QTSPs in order to ensure non-repudiation, facilitate audits, and provide legal certainty in electronic transactions. To resolve any apparent contradiction with general data minimisation principles, we disclose these overriding mandates transparently:

- **Qualified Certificates and Certificate-Holder Identification Data —** retained for 10 years from the end of the certificate's validity, to guarantee service continuity and provide undeniable proof of certification in the event of judicial disputes over electronic signatures.
- **Automatic Validation Logs for Electronic Signatures and Seals —** retained for 3 years.
- **Remote Video Identity Proofing Recordings (including rejected onboarding sessions) —** retained for 3 years from the date of recording in order to satisfy internal audit requirements and external regulatory controls.

This extended processing is strictly ring-fenced for legal compliance and dispute resolution purposes. It is never used for commercial profiling.

6. Cybersecurity and NIS2 Incident Notifications

Under Directive (EU) 2022/2555 (NIS2), Centrul de Calcul SA is classified as an "essential entity" by virtue of its status as a Trust Service Provider. We are therefore subject to the highest tier of cybersecurity risk-management and reporting obligations defined in European law.

6.1 Risk Management Measures (NIS2 Article 21)

We deploy state-of-the-art technical and organisational measures to manage security risk, including:

- Enforced cyber hygiene practices and mandatory security training for all personnel;
- Strong, modern cryptography for data at rest and data in transit;
- Multi-factor authentication (MFA) for every administrative and privileged access path;
- Rigorous supply chain security, including assessment of all sub-processors;
- Continuous monitoring, intrusion detection, and incident response capabilities;
- Alignment with the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) in addition to compliance with GDPR Article 32.

6.2 User-Facing Incident Notification (NIS2 Article 23)

The NIS2 Directive expands the incident notification paradigm beyond mere data breaches: it covers any significant cybersecurity incident that is likely to adversely affect the provision of our services. Where applicable, Article 23(2) requires us to inform the recipients of our services — that is, you — of any actionable cyber threat and of the specific measures or remedies you can take to protect yourself.

We follow the multi-stage reporting cadence mandated by NIS2:

- **24-hour Early Warning —** Within 24 hours of becoming aware of a significant cybersecurity incident, we issue an initial notification to the competent national authority (CSIRT) and, where applicable, to affected users through direct email, immediate in-app dashboard alerts, or a public service announcement.
- **72-hour Detailed Notification —** Within 72 hours we provide a detailed technical assessment of the incident, confirm or deny the presence of a personal data breach under GDPR Article 34, and communicate specific self-protection measures to affected users.
- **One-Month Final Report —** Within one month we publish a comprehensive final report describing the root cause, the mitigation measures deployed, and the preventive actions taken.

This structured incident communication transforms the present Policy into an active component of our incident response and crisis communication strategy.

7. Data Sharing, Sub-processors, and International Transfers

We only share personal data with carefully vetted third parties and only to the extent necessary for the delivery of the services you have requested or for the fulfilment of a legal obligation.

7.1 Categories of Recipients

- Cloud hosting and infrastructure providers (for example AWS, Microsoft Azure) operating within the European Union;
- Payment service providers and payment gateways for the processing of invoices and subscriptions;
- External analytics and monitoring services used to ensure security, stability, and performance;
- Professional advisers (auditors, accountants, lawyers) under strict confidentiality obligations;
- Competent supervisory and judicial authorities (including the ANSPDCP, DNSC, and law-enforcement agencies) where a binding legal obligation applies.

7.2 Sub-processor Transparency

We maintain a regularly updated schedule of sub-processors for each product family, describing the nature of the data shared with each sub-processor and providing direct links to their respective privacy policies. This schedule is available on request through the Privacy Dashboard (for EUDI Wallet users), through the SaaS administration console (for corporate clients), or by written request to the DPO.

7.3 International Transfers Outside the EEA

Where data is transferred to a country outside the European Economic Area, we rely exclusively on a valid legal transfer mechanism recognised by the GDPR:

- A European Commission adequacy decision;
- Standard Contractual Clauses (SCCs) complemented by a documented Transfer Impact Assessment;
- Binding Corporate Rules, where available;
- One of the specific derogations of Article 49 of the GDPR, used restrictively.

8. Application-Specific Policies (Modular Chapters)

The sections above constitute the universal baseline that applies to every Centrul de Calcul product. The following modular chapters address the distinct architectural realities and third-party regulatory environments of each application family.

8.1 Mobile Applications (iOS and Android)

Our mobile applications comply with both the GDPR and the pseudo-regulatory frameworks enforced by Apple (App Store) and Google (Play Store).

8.1.1 Alignment with App Store Declarations

- **Google Data Safety —** Our Play Store listing fully discloses whether each data point is collected, shared, or encrypted in transit, and whether collection is optional or mandatory. The legal text of this Policy is reconciled exactly with the declarations submitted to Google Play.
- **Apple Privacy Manifest —** Every iOS application bundle contains the PrivacyInfo.xcprivacy file, which cryptographically declares the exact data types collected and justifies the use of "Required Reason APIs". This declaration mirrors the taxonomy used in this Policy (e.g. precise location, approximate location, health data, financial information, device identifiers).

8.1.2 SDKs, Permissions, and Consent

No analytics, advertising, or tracking SDK is initialised before you give affirmative consent through our consent banner. The operating-system-level permissions our apps may request (camera, microphone, precise location, notifications) are transparently mapped to the specific processing purpose that justifies them.

8.1.3 In-App Account Deletion

In line with the Apple and Google requirements, every mobile application that offers account creation also provides an intuitive in-app account deletion function. When you request deletion, we confirm the action, execute it, and permanently purge your account from our backend cloud servers within a grace period that is disclosed to you at the moment of the request.

8.2 Web-Based SaaS and Cloud Platforms

8.2.1 Controller vs Processor Roles

For our SaaS platforms, our legal posture shifts depending on the use case:

- **Data Processor —** When a corporate client uses our SaaS platform to process the personal data of its own end-users, employees, or constituents, Centrul de Calcul SA acts strictly as a Data Processor. Customer data is processed exclusively on the basis of the

executed Data Processing Agreement (DPA) and the documented instructions of the client, who retains the Controller role.

- **Independent Data Controller —** When Centrul de Calcul SA aggregates telemetry or metadata from the SaaS platform to analyse performance, optimise architecture, or improve the service, we act as an independent Controller for that specific data stream. This activity is subject to a separate lawful basis and is transparently disclosed in this Policy.

8.2.2 Multi-Tenant Isolation

Our multi-tenant architecture is engineered to guarantee the logical isolation of each tenant's data. Robust access-control policies structurally prevent cross-tenant data leakage, and all critical operations — data export, backup recovery, and deletion — function strictly on an isolated, tenant-by-tenant basis.

8.2.3 Cookies and Tracking Technologies (Law No. 506/2004)

Romanian Law No. 506/2004, which transposes the ePrivacy Directive, strictly prohibits the installation of any non-essential cookie, local storage object, or similar tracking technology without your prior, explicitly informed consent. No analytical or marketing tracking script is initialised on our websites until you have proactively opted in. We do not use pre-ticked boxes or any form of implied consent.

Our dedicated Cookie Policy categorises every tracker in use — strictly essential, performance analytics, functional, and marketing — and explains its retention period. The ANSPDCP has imposed significant fines for cookie violations (approximately 37,000 RON on individuals and up to 100,000 RON on corporations) and our practices are designed to align strictly with those enforcement precedents.

Traffic and location data are retained exclusively for the period necessary to transmit the communication or for billing purposes, and are deleted or anonymised thereafter, unless you have given explicit consent for the provision of value-added services.

8.3 Desktop Software and Telemetry Operations

8.3.1 Local Storage Responsibility

Certain desktop applications are designed to store data entirely locally on your hard drive, with no external transmission to the servers of Centrul de Calcul SA. In these deployments, Centrul de Calcul SA possesses no technical access to, or control over, the locally siloed data. The responsibility for device-level data protection — full-disk encryption, endpoint detection and response, and local access control — rests with you (for consumer deployments) or with your employing organisation (for enterprise deployments).

8.3.2 Telemetry and Opt-In Consent

Where a desktop application transmits telemetry — usage statistics, error logs, or performance metrics — back to us, we rely on the lawful basis of legitimate interest under Article 6(1)(f) of the GDPR, supported by a documented balancing test. You can inspect a summary of this test on request.

8.3.3 Crash Reporting and Anonymisation

Crash reporting is subject to a separate, explicit opt-in mechanism, because automated crash dumps can inadvertently capture segments of system memory that may contain highly sensitive personal data, passwords, or confidential documents. On receipt, all telemetry data is subjected to documented pseudonymisation or anonymisation routines that strip direct identifiers, so that performance analytics cannot be reverse-engineered to identify a specific user or device.

9. Data Subject Rights and Exercise Mechanisms

Under the GDPR you benefit from a suite of rights that we actively support. You may exercise any of these rights free of charge by contacting our DPO (dpo@centruldecalcul.ro) or, for EUDI Wallet users, by using the relevant function of the built-in Privacy Dashboard.

9.1 Your Rights

- **Right of Access (Article 15) —** You can obtain confirmation that we are processing your personal data and request a copy of that data.
- **Right to Rectification (Article 16) —** You can ask us to correct inaccurate personal data.
- **Right to Erasure (Article 17) —** You can ask us to delete personal data, subject to our QTSP legal retention mandates.
- **Right to Restriction (Article 18) —** You can ask us to pause processing while a dispute is resolved.
- **Right to Data Portability (Article 20) —** You can receive your data in a structured, commonly used, machine-readable format and transmit it to another controller.
- **Right to Object (Article 21) —** You can object, on grounds relating to your particular situation, to processing based on legitimate interest.
- **Rights in Relation to Automated Decision-Making (Article 22) —** Where automated decision-making or profiling is used, we will provide meaningful information about the logic involved, the significance, and the envisaged consequences of such processing, and you may request human intervention.
- **Right to Withdraw Consent —** Where processing is based on consent you may withdraw that consent at any time, without affecting the lawfulness of processing carried out prior to the withdrawal.

9.2 How to Exercise Your Rights

- Step 1 — Submit your request via email to dpo@centruldecalcul.ro or via the in-product controls (Privacy Dashboard for the EUDI Wallet; in-app deletion for mobile applications; admin console for SaaS);
- Step 2 — We will confirm receipt within three (3) working days and, where necessary, ask you to verify your identity through a minimised verification flow;
- Step 3 — We will respond substantively within one (1) month. This period may be extended by a further two (2) months where the request is complex, in which case you will be informed in advance.

9.3 Right to Lodge a Complaint

You always retain the right to lodge a formal complaint with the Romanian supervisory authority:

- **Authority:** Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)
- **Address:** B-dul G-ral. Gheorghe Magheru 28-30, Sector 1, 010336 Bucharest, Romania
- **Website:** www.dataprotection.ro

10. Policy Lifecycle and Updates

10.1 Versioning Strategy

This Policy is subject to versioned revisions. Every revision is dated, numbered, and archived so that you can review previous versions on request. Editorial adjustments that do not alter the meaning of the text are released as minor versions; material changes to data-handling practices or to regulatory alignment are released as major versions.

10.2 Current Version

- **Version:** 1.1 (3 November 2026 – editorial change: the “Public” classification label in the page footer and the statement on the document language, as the Romanian and English versions are published separately; the meaning of the text is unchanged)
- **Effective Date:** 20 April 2026
- **Review Cadence:** annual, or sooner in case of significant regulatory or architectural change

10.3 Notification of Material Changes

Where we introduce a material change — for example a new category of data, a new sub-processor of strategic importance, a new cross-border transfer mechanism, or a new application family — we will notify you in advance through:

- Direct email to the address associated with your account;
- In-app pop-up notifications when you next open the application;
- A clearly visible banner on our public website and, where applicable, the EUDI Wallet Privacy Dashboard.

The updated Policy will only enter into force after an appropriate notice period and, where the change requires fresh consent under the GDPR, we will ask you to renew your consent before the change takes effect.

End of the English version.