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: 1.0

Document Language: English (Part I) — Romanian (Part II)

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:** 1.0
- **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. The Romanian version follows on the next page.

Politica Generală de Confidențialitate

Centrul de Calcul SA

Prestator de Servicii de Încredere Calificate (QTSP)
Candidat — Acreditare Portofel European de Identitate Digitală (EUDI)

Data intrării în vigoare: 20 aprilie 2026
Versiune: 1.0
Limba documentului: Engleză (Partea I) — Română (Partea II)

Preambul

Prezenta Politică Generală de Confidențialitate (denumită în continuare „Politica”) descrie modul în care Centrul de Calcul SA („Centrul de Calcul”, „noi” sau „societatea”) colectează, utilizează, stochează și protejează datele dumneavoastră cu caracter personal prin intermediul aplicațiilor mobile, platformelor Software-as-a-Service (SaaS), aplicațiilor desktop, al Portofelului European de Identitate Digitală (EUDI) și al Serviciilor de Încredere Calificate pe care le operează.

Am redactat această Politică pentru a îndeplini cerințele de transparență ale articolului 12 din Regulamentul general privind protecția datelor (GDPR). Este scrisă într-un limbaj clar și simplu și este organizată ca un document modular: un fundament universal aplicabil tuturor produselor, urmat de capitole dedicate fiecărei familii de produse.

Centrul de Calcul SA a fost înființat în România în anul 1976 și operează ca Prestator de Servicii de Încredere Calificate în temeiul Regulamentului (UE) nr. 910/2014 (eIDAS). În prezent, societatea se află în procedura de acreditare pentru serviciile de Portofel EUDI în temeiul Regulamentului (UE) 2024/1183 (eIDAS 2.0). Prelucrarea datelor cu caracter personal este guvernată suplimentar de Legea nr. 190/2018, Legea nr. 506/2004 și Directiva (UE) 2022/2555 (NIS2), alături de Cadrul de Securitate Cibernetică NIST.

1. Introducere, Domeniu de Aplicare și Definiții

1.1 Operatorul de Date

Operatorul datelor cu caracter personal prelucrate în legătură cu serviciile descrise în prezenta Politică este:

- **Denumire legală:** Centrul de Calcul SA
- **Sediu social:** Târgu Jiu, Gorj, România
- **Contact principal:** privacy@centruldecalcul.ro
- **Website:** https://centruldecalcul.ro
- **Website:** https://certdigital.ro

1.2 Domeniul de Aplicare al Politicii

Prezenta Politică se aplică oricărei interacțiuni pe care o aveți cu Centrul de Calcul SA prin următoarele categorii de produse și servicii:

- Aplicații mobile distribuite prin Apple App Store și Google Play Store;
- Platforme Software-as-a-Service (SaaS) furnizate de pe centruldecalcul.ro și subdomeniile asociate;

- Software desktop și aplicații client on-premises instalate pe stația dumneavoastră de lucru sau în rețeaua internă a organizației;
- Portofelul European de Identitate Digitală (EUDI) și Serviciile de Încredere Calificate asociate (certificate calificate, semnături și sigilii electronice calificate, mărci temporale calificate, servicii de validare și conservare calificate, identificare video la distanță).

1.3 Definiții

Pentru ca Politica să fie inteligibilă pentru orice cititor, termenii-cheie au înțelesul de mai jos:

- **Date cu Caracter Personal —** Orice informație privind o persoană fizică identificată sau identificabilă.
- **Operator —** Entitatea care stabilește scopurile și mijloacele prelucrării.
- **Persoană Împuternicită —** Un terț care prelucrează date cu caracter personal în numele și pe baza instrucțiunilor stricte ale Operatorului.
- **Prestator de Servicii de Încredere Calificate (QTSP) —** Entitate acreditată în baza eIDAS să furnizeze servicii electronice de încredere calificate.
- **Parte Utilizatoare (Relying Party) —** Orice entitate publică sau privată care solicită, primește sau validează informații din Portofelul EUDI.
- **Portofel EUDI —** Portofelul European de Identitate Digitală definit prin Regulamentul (UE) 2024/1183.
- **CNP —** Codul numeric personal, identificator național atribuit fiecărui cetățean român.
- **ANSPDCP —** Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

2. Supraveghere: Responsabilul cu Protecția Datelor (DPO)

Întrucât serviciile Centrului de Calcul SA implică prelucrarea la scară largă a unor identificatori naționali și a altor date sensibile, am desemnat un Responsabil cu Protecția Datelor (DPO), în conformitate cu articolul 37 din GDPR și cu articolul 10 din Legea nr. 190/2018.

2.1 Datele de Contact ale DPO

- **E-mail:** dpo@centruldecalcul.ro
- **Adresă poștală:** Responsabil cu Protecția Datelor, Centrul de Calcul SA, Târgu Jiu, Gorj, România

Puteți contacta DPO direct și confidențial cu privire la orice aspect referitor la prelucrarea datelor dumneavoastră sau la exercitarea drepturilor conferite de GDPR.

2.2 Supravegherea DPO asupra Codului Numeric Personal (CNP)

În calitatea noastră de QTSP suntem obligați să colectăm și să prelucrăm Codul Numeric Personal (CNP), seria și numărul cărții de identitate și numărul pașaportului, pentru emiterea certificatelor calificate și operarea Portofelului EUDI. Articolul 4 din Legea nr. 190/2018 impune condiții stricte pentru prelucrarea acestor identificatori naționali.

Atunci când invocăm interesul legitim al operatorului, în temeiul articolului 6 alineatul (1) litera (f) din GDPR, pentru a prelucra CNP-ul, Legea nr. 190/2018 impune desemnarea obligatorie a unui DPO și implementarea unor garanții dedicate. În consecință, DPO exercită o supraveghere specifică, documentată, asupra următoarelor:

- Colectarea, stocarea și utilizarea CNP-ului și a identificatorilor naționali asociați;
- Controlul accesului și jurnalizarea de audit pentru orice interogare internă a acestor identificatori;
- Durata de stocare și ștergerea securizată a acestor identificatori la finalul perioadei de păstrare;
- Evaluarea oricărei propuneri de nouă activitate de prelucrare care ar implica CNP-ul, înainte de punerea acesteia în funcțiune.

Prin această supraveghere dedicată ne asigurăm că identificatorii naționali, extrem de sensibili, sunt supuși unei supravegheri reglementare interne mai stricte decât orice altă categorie de date cu caracter personal.

3. Principiile Universale de Prelucrare a Datelor

Fiecare echipă de inginerie, echipă de operațiuni și terț care acționează în numele nostru este obligat să respecte următoarele principii fundamentale ale GDPR, integrate în arhitectura fiecărui produs:

- **Legalitate, Echitate și Transparență —** Prelucrăm date cu caracter personal doar atunci când există un temei legal identificat și vă comunicăm întotdeauna modul în care le utilizăm.
- **Limitarea Scopului —** Colectăm datele pentru scopuri determinate, explicite și legitime și nu le prelucrăm ulterior într-un mod incompatibil cu acestea.
- **Minimizarea Datelor —** Colectăm strict ce este necesar furnizării serviciului solicitat, acordând o atenție deosebită mecanismului de divulgare selectivă din Portofelul EUDI.
- **Exactitate —** Luăm toate măsurile rezonabile pentru a menține datele exacte și actualizate și vă oferim mijloacele de a le corecta.
- **Limitarea Stocării —** Păstrăm datele doar atât cât este necesar scopurilor prelucrării, sub rezerva perioadelor legale de păstrare specifice activităților QTSP.

- **Integritate și Confidențialitate —** Protejăm datele prin criptografie de ultimă generație, control strict al accesului, autentificare multi-factor, jurnalizare monitorizată și detectare continuă a amenințărilor.
- **Responsabilitate —** Documentăm și auditam în mod continuu conformitatea cu fiecare dintre principiile de mai sus și cu orice obligație legală aplicabilă.

4. Categoriile de Date Colectate și Temeiurile Legale ale Prelucrării

Matricea de mai jos asociază fiecare categorie de date cu caracter personal pe care o colectăm elementelor reprezentative, scopului prelucrării și temeiului legal aplicabil conform GDPR. Atunci când sunt implicate categorii speciale de date (de exemplu, date biometrice sau de sănătate), ne întemeiem pe articolul 9 alineatul (2) litera (a) din GDPR și pe articolul 3 din Legea nr. 190/2018, ambele impunând consimțământul dumneavoastră explicit și neechivoc sau o prevedere legală expresă, dublată de garanții adecvate.

Categoria de Date	Elemente Reprezentative	Scopul Prelucrării	Temei Legal (GDPR)
Cont și Identitate de Bază	Nume, adresă de e-mail, CNP, număr de telefon	Furnizarea serviciului, administrarea contului, verificarea identității QTSP	Art. 6(1)(b) Contract; Art. 6(1)(c) Obligație Legală; Art. 6(1)(f) Interes Legitim
Date Financiare și de Facturare	Adresă de facturare, istoric plăți, tranzacții	Administrarea abonamentelor, facturare, conformitate financiară	Art. 6(1)(b) Contract; Art. 6(1)(c) Obligație Legală
Date Tehnice și de Dispozitiv	Adresă IP, sistem de operare, identificatori unici de dispozitiv	Monitorizare de securitate, prevenirea fraudei, analize de stabilitate software	Art. 6(1)(f) Interes Legitim
Date Biometrice	Vectori faciali generați în procesul de înrolare	Identificare la distanță pentru emiterea Serviciilor de Încredere Calificate	Art. 9(2)(a) Consimțământ Explicit
Date din Categorii Speciale	Date de sănătate, apartenență sindicală (dacă se aplică unor aplicații specifice)	Furnizarea unor module software specializate	Art. 9(2)(a) Consimțământ Explicit sau derogări legale specifice

4.1 Interesul Legitim și Testul de Echilibru

Oriunde invocăm articolul 6 alineatul (1) litera (f) din GDPR — de exemplu pentru telemetrie software, analize de securitate sau prevenirea fraudei — am efectuat și documentat un test de echilibru care demonstrează că interesele comerciale ale Centrului de Calcul SA nu prevalează asupra drepturilor și libertăților dumneavoastră fundamentale. Puteți solicita un rezumat al acestei evaluări trimițând o cerere la DPO.

4.2 Categorii Speciale de Date și Consimțământul Explicit

Prelucrarea biometrică ce permite identificarea video la distanță pentru emiterea certificatelor calificate, precum și orice prelucrare de categorie specială din cadrul aplicațiilor specializate, se întemeiază întotdeauna pe consimțământul dumneavoastră explicit. Acest consimțământ este solicitat separat, descris granular și poate fi retras în orice moment.

5. Servicii de Încredere și Dispoziții Specifice eIDAS 2.0

Portofelul EUDI oferit de Centrul de Calcul SA este proiectat conform Regulamentului (UE) 2024/1183 (eIDAS 2.0) și operaționalizează principiile GDPR privind protecția datelor începând cu momentul conceperii și în mod implicit direct în arhitectura sa criptografică.

5.1 Controlul Exclusiv al Utilizatorului și Stocarea Locală

Păstrați controlul unic și exclusiv asupra Portofelului European de Identitate Digitală. Datele de Identificare Personală (PID) și Atestările Electronice de Atribute (EAA) — precum permisul de conducere mobil, acreditările de studii sau atestările financiare — sunt stocate local, pe hardware-ul securizat al dispozitivului (de exemplu, secure enclave-ul telefonului mobil). Acestea nu sunt stocate pe servere centrale operate de Centrul de Calcul SA sau de statul român.

5.2 Divulgare Selectivă și Dovezi cu Cunoștințe Zero (ZKP)

Portofelul integrează tehnologii avansate de consolidare a confidențialității — Divulgare Selectivă și Dovezi cu Cunoștințe Zero (Zero-Knowledge Proofs / ZKP) — care vă permit să transmiteți exclusiv atributele granulare solicitate de o Parte Utilizatoare, fără a dezvălui întregul document.

De exemplu, puteți demonstra criptografic faptul că aveți peste 18 ani fără a dezvălui data exactă de naștere, numele sau adresa. În acest fel reducem suprafața de atac pentru frauda de identitate și aplicăm principiul minimizării datelor la nivel de protocol.

5.3 Neconectabilitate și Inobservabilitate

În temeiul articolului 5a din Regulamentul (UE) 2024/1183, Portofelul garantează proprietățile de neconectabilitate și inobservabilitate. Noi, în calitate de furnizor al Portofelului, suntem incapabili, atât tehnic, cât și procedural, să urmărim, să observăm sau să profilăm interacțiunile sau tranzacțiile dumneavoastră.

Arhitectura asigură că nici furnizorul Portofelului, nici emitentul original al acreditării nu primește vreo notificare sau telemetrie atunci când prezentați un document unei Părți Utilizatoare. Această inobservabilitate criptografică împiedică alcătuirea de profiluri comportamentale și vă protejează împotriva supravegherii.

5.4 Separarea Seturilor de Date QTSP

În temeiul articolului 45h din eIDAS 2.0, datele de identitate generate prin Serviciile de Încredere Calificate sunt separate logic și organizațional de orice alt set de date produs prin alte servicii comerciale oferite de Centrul de Calcul SA. Este strict interzisă combinarea, corelarea sau agregarea datelor de identitate din serviciile de încredere cu date de marketing, telemetrie sau cu orice alt set de date comerciale.

5.5 Tabloul de Bord de Confidențialitate Integrat

Portofelul include un tablou de bord (Privacy Dashboard) cuprinzător, orientat către utilizator, care constituie punctul unic de control. Din tabloul de bord puteți:

- Consulta un jurnal complet și actualizat al atributelor divulgate și al Părților Utilizatoare destinatare;
- Revizui registrul Părților Utilizatoare cu care ați interacționat și revoca accesele viitoare;
- Transmite o Cerere de Ștergere a Datelor direct către o Parte Utilizatoare (specificație EC TS07 v1.0), în temeiul articolului 17 din GDPR;
- Transmite o Plângere privind o solicitare nelegală sau suspectă direct către ANSPDCP (specificație EC TS08 v0.95), din cadrul aplicației;
- Verifica identitatea criptografică și statutul juridic al oricărei Părți Utilizatoare prin intermediul interfeței „Trust Mark UI view”.

Înainte de orice transmisie, Portofelul evaluează politica de confidențialitate încorporată într-un format inteligibil mașină — adesea exprimată în limbajul Digital Credentials Query Language (DCQL) — pe care Partea Utilizatoare a inclus-o în cerere, astfel încât să puteți aproba sau refuza solicitarea fiind pe deplin informat asupra scopului acesteia.

5.6 Obligații de Păstrare Specifice QTSP ce Prevalează

În timp ce GDPR pune accent pe limitarea stocării, eIDAS și legislația națională română impun QTSP-urilor perioade de păstrare specifice și extinse, pentru a asigura non-repudierea, a facilita auditul și a oferi certitudine juridică în tranzacțiile electronice. Pentru a rezolva aparenta contradicție cu principiul minimizării datelor, vă comunicăm în mod transparent aceste obligații prevalente:

- **Certificate Calificate și Date de Identificare ale Titularului —** păstrate pentru 10 ani de la data expirării certificatului, pentru a garanta continuitatea serviciului și a furniza dovezi incontestabile de certificare în eventualele litigii privind semnăturile electronice.

- **Jurnale de Validare Automată a Semnăturilor și Sigiliilor Electronice —** păstrate pentru 3 ani.
- **Înregistrări ale Sesiunilor de Identificare Video la Distanță (inclusiv cele respinse) —** păstrate pentru 3 ani de la data înregistrării, pentru a respecta cerințele interne de audit și controalele externe de reglementare.

Această prelucrare extinsă este strict circumscrisă conformității juridice și soluționării litigiilor. Nu este niciodată utilizată pentru profilare comercială.

6. Securitatea Cibernetică și Notificarea Incidentelor NIS2

În temeiul Directivei (UE) 2022/2555 (NIS2), Centrul de Calcul SA este clasificată drept „entitate esențială" în virtutea statutului său de Prestator de Servicii de Încredere. Prin urmare, suntem supuși celui mai înalt nivel de obligații privind managementul riscului și raportarea incidentelor, prevăzut de dreptul european.

6.1 Măsuri de Management al Riscului (Art. 21 NIS2)

Implementăm măsuri tehnice și organizatorice de ultimă generație pentru gestionarea riscurilor de securitate, inclusiv:

- Practici obligatorii de igienă cibernetică și instruire de securitate pentru întregul personal;
- Criptografie robustă, modernă, pentru datele în repaus și în tranzit;
- Autentificare multi-factor (MFA) pentru orice acces administrativ sau privilegiat;
- Securitate riguroasă a lanțului de aprovizionare, inclusiv evaluarea tuturor persoanelor împuternicite;
- Monitorizare continuă, detectare a intruziunilor și capacități de răspuns la incidente;
- Aliniere cu Cadrul de Securitate Cibernetică NIST (Identify, Protect, Detect, Respond, Recover), în plus față de conformitatea cu articolul 32 din GDPR.

6.2 Notificarea Incidentelor către Utilizatori (Art. 23 NIS2)

Directiva NIS2 extinde paradigma de notificare a incidentelor dincolo de simplele încălcări ale securității datelor: acoperă orice incident semnificativ de securitate cibernetică susceptibil să afecteze negativ furnizarea serviciilor noastre. Acolo unde este aplicabil, articolul 23 alineatul (2) ne obligă să informăm destinatarii serviciilor — adică pe dumneavoastră — cu privire la orice amenințare cibernetică care necesită acțiune imediată și la măsurile sau remediile pe care le puteți lua pentru a vă proteja.

Respectăm cadența de raportare în mai multe etape impusă de NIS2:

- **Avertizare Timpurie în 24 de ore —** În termen de 24 de ore de la momentul în care luăm cunoștință de un incident semnificativ de securitate cibernetică, transmitem o notificare

inițială autorității naționale competente (CSIRT) și, acolo unde este cazul, utilizatorilor afectați, prin e-mail direct, alerte imediate în tabloul de bord al aplicației sau printr-un comunicat public.

- **Notificare Detaliată în 72 de ore —** În termen de 72 de ore furnizăm o evaluare tehnică detaliată a incidentului, confirmăm sau infirmăm existența unei încălcări a securității datelor în sensul articolului 34 din GDPR și comunicăm utilizatorilor afectați măsuri concrete de auto-protecție.
- **Raport Final în Termen de o Lună —** În termen de o lună publicăm un raport final cuprinzător, descriind cauza primară, măsurile de atenuare aplicate și acțiunile preventive.

Această comunicare structurată a incidentelor transformă prezenta Politică într-o componentă activă a strategiei noastre de răspuns la incidente și de comunicare în situații de criză.

7. Partajarea Datelor, Persoane Împuternicite și Transferuri Internaționale

Partajăm date cu caracter personal doar cu terți atent selectați și doar în măsura necesară pentru livrarea serviciilor solicitate sau pentru îndeplinirea unei obligații legale.

7.1 Categorii de Destinatari

- Furnizori de găzduire și infrastructură cloud (de exemplu AWS, Microsoft Azure) care operează pe teritoriul Uniunii Europene;
- Prestatori de servicii de plată și gateway-uri de plată pentru procesarea facturilor și abonamentelor;
- Servicii externe de analiză și monitorizare utilizate pentru asigurarea securității, stabilității și performanței;
- Consultanți profesionali (auditori, contabili, avocați) supuși unor obligații stricte de confidențialitate;
- Autorități de supraveghere și autorități judiciare competente (inclusiv ANSPDCP, DNSC și organe de aplicare a legii) atunci când există o obligație legală.

7.2 Transparență privind Persoanele Împuternicite

Menținem o listă actualizată periodic a persoanelor împuternicite pentru fiecare familie de produse, descriind natura datelor partajate și furnizând link-uri directe către politicile lor de confidențialitate. Această listă este disponibilă la cerere prin tabloul de bord de confidențialitate (pentru utilizatorii Portofelului EUDI), prin consola de administrare SaaS (pentru clienții corporativi) sau prin cerere scrisă transmisă DPO.

7.3 Transferuri Internaționale în Afara SEE

Atunci când datele sunt transferate către o țară din afara Spațiului Economic European, ne întemeiem exclusiv pe un mecanism juridic valabil de transfer recunoscut de GDPR:

- O decizie de adecvare a Comisiei Europene;
- Clauze Contractuale Standard (CCS) completate de o Evaluare Documentată a Impactului Transferului;
- Reguli Corporative Obligatorii, acolo unde sunt disponibile;
- Una dintre derogările specifice ale articolului 49 din GDPR, utilizată în mod restrictiv.

8. Politici Specifice pe Aplicații (Capitole Modulare)

Secțiunile de mai sus constituie fundamentul universal aplicabil fiecărui produs al Centrului de Calcul SA. Capitolele modulare de mai jos abordează realitățile arhitecturale distincte și cerințele reglementare specifice fiecărei familii de aplicații.

8.1 Aplicații Mobile (iOS și Android)

Aplicațiile noastre mobile respectă atât GDPR-ul, cât și cadrele pseudo-reglementare impuse de Apple (App Store) și Google (Play Store).

8.1.1 Corelarea cu Declarațiile din Magazinele de Aplicații

- **Google Data Safety —** Listarea noastră în Play Store declară în totalitate dacă fiecare tip de date este colectat, partajat sau criptat în tranzit și dacă respectiva colectare este opțională sau obligatorie. Textul juridic al prezentei Politici este aliniat exact cu declarațiile transmise către Google Play.
- **Apple Privacy Manifest —** Fiecare pachet de aplicație iOS conține fișierul PrivacyInfo.xcprivacy, care declară criptografic tipurile exacte de date colectate și justifică utilizarea „API-urilor cu motiv obligatoriu”. Această declarație oglindește taxonomia utilizată în prezenta Politică (de exemplu, locație precisă, locație aproximativă, date de sănătate, informații financiare, identificatori de dispozitiv).

8.1.2 SDK-uri, Permisiuni și Consimțământ

Niciun SDK de analiză, publicitate sau urmărire nu este inițializat înainte de acordarea consimțământului afirmativ prin banner-ul nostru de consimțământ. Permisiunile la nivel de sistem de operare pe care aplicațiile le pot solicita (cameră, microfon, locație precisă, notificări) sunt asociate transparent scopului specific de prelucrare care le justifică.

8.1.3 Ștergerea Contului din Aplicație

Conform cerințelor Apple și Google, orice aplicație mobilă care permite crearea unui cont oferă și o funcție intuitivă de ștergere a contului din aplicație. Atunci când solicitați ștergerea, confirmăm acțiunea, o executăm și eliminăm definitiv contul din serverele noastre cloud într-un termen de grație comunicat în momentul solicitării.

8.2 SaaS Web și Platforme Cloud

8.2.1 Rolurile de Operator vs. Persoană Împuternicită

Pentru platformele noastre SaaS, poziția noastră juridică se modifică în funcție de caz:

- **Persoană Împuternicită —** Atunci când un client corporativ utilizează platforma SaaS pentru a prelucra datele cu caracter personal ale propriilor utilizatori finali, angajați sau alegători, Centrul de Calcul SA acționează strict în calitate de persoană împuternicită. Datele clientului sunt prelucrate exclusiv pe baza Acordului de Prelucrare a Datelor (DPA) încheiat și pe instrucțiunile documentate ale clientului, care păstrează rolul de Operator.
- **Operator Independent —** Atunci când Centrul de Calcul SA agregă telemetrie sau metadate din platforma SaaS pentru a analiza performanța, a optimiza arhitectura sau a îmbunătăți serviciul, acționăm în calitate de Operator independent pentru acel flux specific de date. Această activitate se bazează pe un temei legal separat și este divulgată transparent în prezenta Politică.

8.2.2 Izolarea Multi-Tenant

Arhitectura noastră multi-tenant este proiectată pentru a garanta izolarea logică a datelor fiecărui client. Politicile robuste de control al accesului previn structural scurgerile de date între tenanți, iar toate operațiunile critice — exportul de date, recuperarea din backup și ștergerea — funcționează strict per tenant, într-un mod izolat.

8.2.3 Cookie-uri și Tehnologii de Urmărire (Legea nr. 506/2004)

Legea nr. 506/2004, care transpune Directiva ePrivacy, interzice strict instalarea oricărui cookie neesențial, a obiectelor de stocare locală sau a tehnologiilor similare de urmărire fără consimțământul dumneavoastră prealabil, informat în mod explicit. Niciun script de urmărire analitică sau de marketing nu este inițializat pe site-urile noastre până când nu optați activ pentru utilizarea acestora. Nu folosim căsuțe pre-bifate sau mecanisme de consimțământ implicit.

Politica noastră dedicată privind cookie-urile clasifică fiecare tracker utilizat — strict necesar, analitic de performanță, funcțional și de marketing — și explică durata de păstrare. ANSPDCP a aplicat amenzi semnificative pentru încălcări privind cookie-urile (aproximativ 37.000 RON pentru persoane fizice și până la 100.000 RON pentru societăți), iar practicile noastre sunt proiectate pentru a fi aliniate strict cu aceste precedente.

Datele de trafic și de localizare sunt păstrate exclusiv pe durata necesară pentru transmiterea comunicării sau pentru facturare și sunt șterse sau anonimizate ulterior, cu excepția cazului în care ați dat consimțământ explicit pentru servicii cu valoare adăugată.

8.3 Software Desktop și Operațiuni de Telemetrie

8.3.1 Responsabilitatea pentru Stocarea Locală

Anumite aplicații desktop sunt concepute să stocheze date exclusiv local, pe hard disk-ul dumneavoastră, fără vreo transmisie externă către serverele Centrului de Calcul SA. În aceste implementări, Centrul de Calcul SA nu deține acces tehnic și nici control asupra datelor stocate local în siloz. Responsabilitatea pentru protecția datelor la nivel de dispozitiv — criptarea completă a discului, detecție și răspuns la nivel de endpoint, controlul accesului local — vă revine dumneavoastră (pentru implementările de consum) sau organizației care vă angajează (pentru implementările enterprise).

8.3.2 Telemetria și Consimțământul Opt-In

Atunci când o aplicație desktop transmite telemetrie — statistici de utilizare, jurnale de erori sau metrici de performanță — către noi, ne întemeiem pe temeiul legal al interesului legitim, conform articolului 6 alineatul (1) litera (f) din GDPR, susținut de un test documentat de echilibru. Puteți consulta un rezumat al acestui test la cerere.

8.3.3 Raportarea Erorilor și Anonimizarea

Raportarea erorilor este supusă unui mecanism distinct, explicit, de opt-in, întrucât descărcările automate de avarie (crash dumps) pot captura, fără intenție, segmente din memoria sistemului care pot conține date cu caracter personal extrem de sensibile, parole sau documente confidențiale. La recepție, toate datele de telemetrie sunt supuse unor rutine documentate de pseudonimizare sau anonimizare care elimină identificatorii direcți, astfel încât analizele de performanță să nu poată fi inversate pentru a identifica un anumit utilizator sau dispozitiv.

9. Drepturile Persoanelor Vizate și Mecanisme de Exercitare

În temeiul GDPR beneficiați de o serie de drepturi pe care le susținem activ. Puteți exercita oricare dintre aceste drepturi în mod gratuit, contactând DPO (dpo@centruldecalcul.ro) sau, în cazul utilizatorilor Portofelului EUDI, utilizând funcția corespunzătoare din tabloul de bord de confidențialitate integrat.

9.1 Drepturile Dumneavoastră

- **Dreptul de Acces (Art. 15) —** Puteți obține confirmarea că vă prelucrăm datele și o copie a acestora.
- **Dreptul la Rectificare (Art. 16) —** Puteți solicita corectarea datelor inexacte.
- **Dreptul la Ștergere (Art. 17) —** Puteți solicita ștergerea datelor, sub rezerva obligațiilor legale de păstrare QTSP.
- **Dreptul la Restricționare (Art. 18) —** Puteți solicita întreruperea temporară a prelucrării pe durata soluționării unui diferend.
- **Dreptul la Portabilitate (Art. 20) —** Puteți primi datele într-un format structurat, utilizat în mod curent și citibil automat, pentru a le transmite unui alt operator.

- **Dreptul de Opoziție (Art. 21) —** Vă puteți opune, pentru motive legate de situația dumneavoastră particulară, prelucrării întemeiate pe interes legitim.
- **Drepturi privind Procesul Decizional Automatizat (Art. 22) —** Atunci când utilizăm decizii automatizate sau profilare, vă furnizăm informații semnificative despre logica implicată, importanța și consecințele prelucrării și puteți solicita intervenție umană.
- **Dreptul de a Retrage Consimțământul —** Acolo unde prelucrarea se bazează pe consimțământ, îl puteți retrage în orice moment, fără a afecta legalitatea prelucrării efectuate anterior retragerii.

9.2 Cum Vă Exercitați Drepturile

- Pasul 1 — Transmiteți solicitarea prin e-mail la dpo@centruldecalcul.ro sau prin comenzile din produs (tabloul de bord pentru Portofelul EUDI; ștergere din aplicație pentru aplicațiile mobile; consolă de administrare pentru SaaS);
- Pasul 2 — Vom confirma primirea în termen de trei (3) zile lucrătoare și, dacă este necesar, vă vom solicita verificarea identității printr-un flux de verificare minimizat;
- Pasul 3 — Vom răspunde pe fond în termen de o (1) lună. Această perioadă poate fi prelungită cu încă două (2) luni în cazul cererilor complexe, situație în care veți fi informat în prealabil.

9.3 Dreptul de a Depune o Plângere

Aveți întotdeauna dreptul de a depune o plângere formală la autoritatea de supraveghere din România:

- **Autoritate:** Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)
- **Adresă:** B-dul G-ral. Gheorghe Magheru 28-30, Sector 1, 010336 București, România
- **Website:** www.dataprotection.ro

10. Ciclul de Viață și Actualizarea Politicii

10.1 Strategie de Versionare

Prezenta Politică este supusă unor revizii versionate. Fiecare revizie este datată, numerotată și arhivată, astfel încât să puteți consulta versiunile anterioare la cerere. Ajustările editoriale care nu modifică sensul textului sunt publicate ca versiuni minore; modificările substanțiale ale practicilor de prelucrare sau ale alinierii reglementare sunt publicate ca versiuni majore.

10.2 Versiunea Curentă

- **Versiune:** 1.0

- **Data intrării în vigoare:** 20 aprilie 2026
- **Cadență de Revizuire:** anuală sau mai frecventă, în cazul unor schimbări semnificative de reglementare sau arhitecturale

10.3 Notificarea Modificărilor Substanțiale

Atunci când introducem o modificare substanțială — de exemplu o nouă categorie de date, o nouă persoană împuternicită cu importanță strategică, un nou mecanism de transfer transfrontalier sau o nouă familie de aplicații — vă vom notifica în prealabil prin:

- E-mail direct la adresa asociată contului dumneavoastră;
- Notificări pop-up în aplicație la următoarea deschidere;
- Un banner vizibil pe website-ul nostru public și, acolo unde este cazul, în tabloul de bord al Portofelului EUDI.

Politica actualizată intră în vigoare doar după o perioadă adecvată de preaviz, iar acolo unde modificarea necesită un consimțământ nou conform GDPR, vă vom solicita reînnoirea consimțământului înainte ca aceasta să producă efecte.

Sfârșitul versiunii în limba română.