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: 10 decembrie 2026

Versiune: 2.0

Limba documentului: română (versiunea în limba engleză se publică separat)

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: sediu@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). Identificarea cu prezență fizică se face la sediul nostru, la punctele de lucru sau la partenerii mandatați de noi, care acționează în numele nostru.

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, seria și numărul actului de identitate, copia actului, documentele cererii (împuterniciri, certificate constatatoare, documente profesionale, la cerere)	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

Identificare la Distanță	Înregistrarea video, imaginile actului, fotografia (selfie), raportul de validare, datele consimțământului	Identificare la distanță pentru emiterea Serviciilor de Încredere Calificate	Art. 6(1)(c) Obligație Legală; 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**, inclusiv copiile documentelor și înregistrările sesiunilor de identificare video pe baza cărora s-a emis un certificat — păstrate cel puțin 10 ani de la încetarea valabilității certificatului (expirare sau revocare) (articolul 16 alineatul (2) din Legea nr. 214/2024); sesiunile de identificare video aprobate pe baza cărora nu s-a emis un certificat — 10 ani de la data identificării; sesiunile de identificare video respinse — 3 ani de la data înregistrării. Vectorii faciali calculați pentru compararea automată nu se păstrează după comparare; din sesiune se păstrează, criptat, înregistrarea video, imaginile și rezultatul comparării.
- **Jurnale de Validare Automată a Semnăturilor și Sigiliilor Electronice —** păstrate pentru 3 ani.

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;
- Partenerii mandatați de Centrul de Calcul SA pentru identificarea cu prezență fizică a solicitanților de certificate calificate și de servicii de semnătură la distanță, care prelucrează în numele nostru, ca persoane împuternicite (articolul 28 din GDPR), datele din actul de identitate, copia acestuia, datele de contact și documentele cererii, numai pentru identificare și pentru înregistrarea cererii, pe baza unui contract care le impune confidențialitatea, securitatea datelor și transmiterea dosarelor către noi;
- Autoritatea pentru Digitalizarea României, ca organism de supraveghere a serviciilor de încredere, și organismul de evaluare a conformității, în limitele controalelor și auditurilor prevăzute de Regulamentul (UE) nr. 910/2014; Platforma națională de interoperabilitate, prin care verificăm valabilitatea actelor de identitate ale cetățenilor români (articolul 12 alineatul (8) din Legea nr. 214/2024);
- 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. Lista cuprinde și partenerii mandatați pentru identificare și punctele lor de lucru. Partenerii sunt prezentați și pe https://www.certdigital.ro/parteneri/.

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:** 2.0 (10 noiembrie 2026 – modificare substanțială: partenerii mandatați pentru identificarea cu prezență fizică, ca persoane împuternicite; Autoritatea pentru Digitalizarea României, organismul de evaluare a conformității și Platforma națională de interoperabilitate, ca destinatari ai datelor; categoriile de date de identificare; perioadele de păstrare a datelor de identificare, pe trei categorii, și a datelor biometrice; pagina partenerilor de pe website; adresa de contact principală din §1.1, sediu@centruldecalcul.ro, ca în versiunea în limba engleză)
- **Data intrării în vigoare: 10 decembrie 2026**
- **Cadență de Revizuire:** anuală sau mai frecventă, în cazul unor schimbări semnificative de reglementare sau arhitecturale

- **Versiunea anterioară:** 1.1 (3 noiembrie 2026 – modificare editorială: eticheta de clasificare „Public” în subsolul paginilor și mențiunea privind limba documentului, pentru că versiunile în română și în engleză se publică separat; sensul textului este neschimbat)

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.