POLITICA DE PROTECȚIE A DATELOR CU CARACTER PERSONAL (GDPR POLICY)

OSIRIS INVESTMENT S.R.L. / LaDepozit

Versiune: 3.1 | Revizuire: septembrie 2026

1. Introducere

Începând cu data de 25 mai 2018, se aplică Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 (**„GDPR"**), care stabilește cadrul juridic aplicabil prelucrării datelor cu caracter personal în Uniunea Europeană.

Osiris Investment S.R.L., persoană juridică română, înregistrată la Registrul Comerțului sub nr. J40/8391/2019, cu sediul social în București, Str. Cristian Tell nr. 19, cam. 2, et. 1, ap. 5bis, Sector 1, având cod unic de înregistrare RO 41318860 (**„Operatorul"** sau **„LaDepozit"**), respectă prevederile GDPR și ale Legii nr. 190/2018 și aplică măsuri tehnice și organizatorice adecvate pentru protecția datelor personale.

Operatorul deține marca înregistrată **LaDepozit** și desfășoară activități de punere la dispoziție de spații de depozitare securizate (*self-storage*) și administrare a platformei digitale asociate.

2. Date de contact

E-mail general: contact@ladepozit.ro
Responsabil cu protecția datelor ("DPO"):
Buda Și Asociații S.P.A.R.L. (Buda Partners), reprezentată prin Av. Ștefan Ionuț Buda
E-mail: privacy@ladepozit.ro

3. Scopurile și temeiurile prelucrării

LaDepozit colectează și prelucrează date cu caracter personal în următoarele scopuri:

Scopul prelucrării	Temei juridic (art. 6 GDPR)	Exemple de activități
Încheierea și executarea contractului	art. 6 alin. (1) lit. b)	Crearea contului, rezervarea boxei, semnarea electronică, facturare
Respectarea obligațiilor legale	art. 6 alin. (1) lit. c)	Raportări contabile și arhivare fiscală, potrivit obligațiilor legale aplicabile
Securitatea persoanelor și a bunurilor	art. 6 alin. (1) lit. f)	Supraveghere video (CCTV), control electronic acces
Verificarea identității clienților și prevenirea fraudelor	art. 6 alin. (1) lit. f)	Verificarea identității și păstrarea copiei CI în limitele necesității documentate
Comunicări administrative și suport clienți	art. 6 alin. (1) lit. b) și (f)	Notificări, relații comerciale, răspunsuri la solicitări

Scopul prelucrării	Temei juridic (art. 6 GDPR)	Exemple de activități
Marketing direct (opțional)	art. 6 alin. (1) lit. a)	Newslettere, comunicări promoționale bazate pe consimțământ
Profilare internă și comunicare comercială personalizată (opțional)	art. 6 alin. (1) lit. a) - consimțământ explicit	Analiză internă a comportamentului clienților, segmentare demografică și transmiterea de oferte personalizate, doar pentru persoanele care și-au exprimat acordul explicit. Lipsa consimțământului nu afectează posibilitatea încheierii contractului.
Controlul accesului și verificarea identității reprezentanților desemnați de clienții persoane juridice	art. 6 alin. (1) lit. f) – interes legitim	Verificarea identității persoanelor desemnate de clientul persoană juridică să acționeze în numele acestuia; controlul accesului în spațiile de depozitare; prevenirea accesului neautorizat
Controlul accesului și verificarea identității utilizatorilor efectivi ai spațiilor de depozitare	art. 6 alin. (1) lit. f) – interes legitim	Verificarea identității persoanelor delegate sau autorizate de client să utilizeze efectiv spațiul de depozitare; prevenirea fraudelor; securitatea bunurilor depozitate și a spațiilor

Notă privind interesul legitim: Prelucrarea datelor cu caracter personal ale reprezentanților persoanelor juridice și ale utilizatorilor efectivi ai spațiilor de depozitare în temeiul interesului legitim (art. 6 alin. (1) lit. f) din GDPR) se întemeiază pe necesitatea obiectivă de a controla accesul în spații securizate care conțin bunuri ale terților, de a preveni accesul neautorizat și fraudele, precum și de a proteja interesele legitime ale Operatorului și ale celorlalți clienți. Operatorul a realizat un test al interesului legitim (LIA – Legitimate Interest Assessment) documentat, disponibil la solicitare prin privacy@ladepozit.ro. Interesul legitim al Operatorului nu prevalează asupra drepturilor și libertăților fundamentale ale persoanelor vizate, prelucrarea fiind limitată la datele strict necesare scopului declarat.

Operatorul nu urmărește colectarea unor categorii speciale de date. Eventualele date sensibile surprinse incidental în imagini CCTV sunt protejate corespunzător. Profilarea internă pentru segmentare și comunicări comerciale personalizate poate utiliza numai atributele pentru care persoana vizată a exprimat un consimțământ separat, specific, informat și facultativ. CNP-ul ca identificator și imaginea CI nu sunt utilizate în aceste scopuri; eventualele atribute derivate (vârstă, sex, localitate) se separă de copia CI. Nu se iau decizii bazate exclusiv pe prelucrare automată care produc efecte juridice sau afectează similar semnificativ persoana, în sensul art. 22 GDPR. Înainte de activarea profilării, Operatorul documentează fluxul, datele, retenția, consimțământul și riscurile și actualizează DPIA.

4. Tipurile de date prelucrate

- Date de identificare: nume, prenume, CNP, serie și număr CI, copie CI (stocată securizat), semnătură. Furnizarea datelor de identificare și de contact este necesară pentru încheierea contractului și pentru acordarea accesului în locații; în lipsa lor,

contractul nu poate fi încheiat, respectiv accesul nu poate fi acordat. Datele pentru marketing și profilare sunt facultative.

- Date de contact: e-mail, telefon, adresă.
- Date contractuale și de plată: IBAN, facturi, istoricul plăților, documente contabile.
- Date tehnice: adrese IP, identificatori de sesiune, loguri acces platformă, coduri PIN/card acces.
- Imagini video: înregistrări CCTV din zonele comune și perimetrele LaDepozit.

5. Supravegherea video (CCTV)

LaDepozit utilizează sisteme CCTV exclusiv în scopul asigurării securității persoanelor și bunurilor, prevenirea furturilor și a vandalismului.

Camerele sunt amplasate doar în zonele de acces și spațiile comune, fără instalarea de echipamente în interiorul boxelor.

Imaginile CCTV se păstrează cel mult 30 de zile și se șterg prin suprascriere, cu excepția conservării separate și justificate pentru incidente, litigii ori cereri, conform regulilor de mai jos.

Accesul la înregistrări este limitat la personalul desemnat al Operatorului și la DPO, doar în cazuri justificate (incident de securitate, cerere a autorităților).

Cererile privind imaginile CCTV se analizează individual, potrivit dreptului exercitat. Dacă sunt îndeplinite condițiile art. 17 GDPR și nu se aplică o excepție legală, imaginile se șterg fără întârzieri nejustificate, inclusiv prin anonimizare ireversibilă, după caz. Restricționarea se aplică în condițiile art. 18 GDPR și nu înlocuiește automat ștergerea. Limitările tehnice se documentează și se remediază; ele nu constituie, prin ele însele, un motiv de refuz sau de amânare până la suprascrierea automată. Imaginile necesare soluționării unei cereri de acces sau unui litigiu se conservă separat, cu acces limitat, numai pentru perioada justificată.

Persoanele vizate sunt informate prin pictograme vizibile la intrarea în locații și prin prezenta politică, conform Ghidului 3/2019.

6. Prelucrarea datelor reprezentanților persoanelor juridice și ale utilizatorilor efectivi ai spațiilor de depozitare

Operatorul prelucrează date cu caracter personal ale următoarelor categorii de persoane care nu sunt parte contractuală directă, în contextul activităților de control al accesului și securitate:

1. **Categoria 2 - Reprezentanți / persoane de contact ai clienților persoane juridice:** persoanele fizice desemnate de un client persoană juridică să acționeze în numele acestuia în relația cu LaDepozit (reprezentanți legali, mandatari, persoane de contact).
2. **Categoria 3 - Utilizatori efectivi ai spațiilor de depozitare:** persoanele fizice delegate sau autorizate de un client (persoană fizică sau juridică) să utilizeze efectiv spațiul de

depozitare, inclusiv angajați, colaboratori, reprezentanți sau alte persoane desemnate de client.

Prelucrarea datelor persoanelor din Categoria 2 și Categoria 3 se întemeiază pe **interesul legitim** al Operatorului (art. 6 alin. (1) lit. f) din GDPR), constând în:

- controlul accesului în spații securizate care conțin bunuri ale clienților;
- identificarea și autentificarea persoanelor autorizate să acceseze spațiile și bunurile depozitate;
- prevenirea accesului neautorizat, a furturilor și a fraudelor;
- protecția intereselor legitime ale Operatorului și ale celorlalți clienți. Informarea persoanelor din Categoriile 2 și 3 se realizează prin Politica de protecție a datelor cu caracter personal, disponibilă la https://ladepozit.ro/politica-gdpr/. Dacă datele sunt obținute direct de la persoana vizată, politica îi este pusă la dispoziție la momentul colectării. Dacă datele sunt obținute de la client, politica se comunică într-un termen rezonabil, de cel mult o lună de la obținerea datelor, dar cel târziu la prima comunicare cu persoana vizată sau la prima divulgare către un alt destinatar, dacă acestea intervin mai devreme. Linkul se include în ecranul de colectare a datelor și în e-mailul/SMS-ul cu mijloacele de acces, fără a amâna o informare datorată anterior. Operatorul păstrează dovada comunicării și a versiunii politicii comunicate. Clientul care desemnează persoana are, suplimentar, obligația contractuală de a-i transmite politica înainte de a comunica datele acesteia către LaDepozit; această obligație nu înlocuiește responsabilitatea Operatorului. Nu se utilizează note de informare separate sau declarații distincte de primire pentru aceste categorii. Pentru Categoriile 2 și 3, copia CI și CNP-ul sunt prelucrate în temeiul art. 6 alin. (1) lit. f) GDPR numai în măsura în care necesitatea lor este demonstrată pentru controlul accesului și prevenirea fraudei. CNP-ul poate asigura corelarea stabilă a înregistrărilor aceleiași persoane desemnate de mai mulți clienți sau care își schimbă actul de identitate. Operatorul documentează de ce verificarea identității fără păstrarea copiei, un identificator intern ori seria și numărul CI nu ating în mod suficient scopul concret. Simpla utilitate administrativă sau calitatea de persoană de contact fără acces fizic nu justifică, singure, colectarea copiei CI și a CNP-ului.

7. Prelucrarea datelor aparținând terților aflați în incinta LaDepozit

În cadrul activităților desfășurate, Operatorul poate prelucra date cu caracter personal și ale unor persoane care nu au o relație contractuală directă cu Operatorul („**terți**”), cum ar fi: persoane care însoțesc clienții, vizitatori, reprezentanți ai furnizorilor sau alte persoane aflate ocazional în incinta locațiilor LaDepozit.

Aceste date pot fi prelucrate, în principal, prin intermediul sistemelor de supraveghere video sau în contextul procedurilor de acces și securitate.

Prelucrarea se bazează pe interesul legitim al Operatorului (art. 6 alin. (1) lit. f) din GDPR, respectiv protejarea persoanelor și a bunurilor, menținerea siguranței în incintă și prevenirea incidentelor.

Accesul în zonele monitorizate video sau în zonele de acces controlat presupune luarea la cunoștință a existenței sistemelor de monitorizare și a scopului acestora, în condițiile afișării vizibile a notelor informative.

8. Stocarea copiilor actelor de identitate (CI)

LaDepozit solicită și păstrează copia actului de identitate numai în măsura necesară și documentată verificării identității, controlului accesului și prevenirii fraudei, pentru categoriile descrise mai sus. Calitatea de persoană de contact fără acces fizic nu justifică singură colectarea CI/CNP.

Copia se colectează prin canale securizate (upload TLS sau scanare controlată) și se păstrează în sistemul intern de document management (DMS). datele se transmit prin conexiuni securizate (TLS) și se stochează în medii protejate, cu acces limitat pe roluri; criptarea la stocare a copiilor CI în DMS și în backupurile aferente este planificată pentru 31 octombrie 2026; măsurile tehnice și organizatorice sunt evaluate și actualizate în raport cu riscurile prelucrării, conform art. 32 GDPR; Accesul este limitat la personalul nominal autorizat din rolurile Vânzări și Contractare; DPO-ul are acces numai în cazuri justificate, în măsura necesară atribuțiilor sale.

Copiile CI ale clienților persoane fizice se păstrează pe durata contractului; păstrarea ulterioară, de cel mult 5 ani de la încetare, este permisă numai în măsura în care necesitatea pentru constatarea, exercitarea sau apărarea unor drepturi este documentată și revizuită periodic. Copiile CI și CNP-ul reprezentanților, persoanelor de contact și utilizatorilor desemnați se păstrează numai pe durata desemnării sau a dreptului de acces și se șterg la încetarea acestuia, cu excepția datelor strict necesare unui incident, litigiu ori unei obligații legale concrete, păstrate separat pe durata justificată. Documentele contractuale și financiar-contabile urmează propriile termene legale, fără extinderea automată a acestora la copiile CI. Copiile reziduale din backup se elimină în cel mult 30 de zile după ștergerea din sistemele active, nu sunt utilizate curent, iar la restaurare se reaplică ștergerile. CNP-ul clienților persoane fizice, inclus în documentele contractuale, urmează termenul de păstrare al acestora (5 ani de la încetarea contractului); datele de marketing și profilare se păstrează până la retragerea consimțământului sau cel mult 2 ani de la ultima interacțiune. Copierea, imprimarea și transmiterea neautorizată a CI prin e-mail/WhatsApp sunt interzise; comunicările necesare exercitării drepturilor se fac prin canale securizate.

CNP-ul ca identificator și imaginea CI nu sunt utilizate pentru profilare sau marketing. Atributele derivate pot fi utilizate numai în condițiile consimțământului separat descris în prezenta politică.

9. Durata de stocare și mecanismele de ștergere

Tip de date	Durată maximă de stocare	Mecanism de ștergere
Documente contractuale	5 ani de la încetarea contractului, sub rezerva termenelor legale speciale aplicabile	Ștergere / anonimizare automată
Date de contact și corespondență	2 ani de la încetarea relației	Ștergere automată CRM
Loguri IT și acces electronic	12 luni	Rotație automată loguri
Imagini CCTV	Maximum 30 de zile; conservare separată numai în cazurile justificate descrise în secțiunea CCTV	Suprascriere automată
Copii CI	Termene diferențiate pentru clienți și persoane desemnate, conform secțiunii „Stocarea copiilor actelor de identitate”; eliminare din backup în cel mult 30 de zile după ștergerea din sistemele active	Ștergere la termen din DMS, de regulă automată și, atunci când automatizarea nu este posibilă, manuală, de către personalul autorizat.

Operatorul verifică periodic respectarea termenelor de retenție. Ștergerea se realizează de regulă automat și, atunci când automatizarea nu este posibilă, manual, de către personalul autorizat, fără prelungirea termenelor aplicabile.

10. Drepturile persoanelor vizate

Persoanele vizate au următoarele drepturi, potrivit GDPR:

- **Dreptul la informare (art. 13–14)**
- **Dreptul de acces (art. 15)**
- **Dreptul la rectificare (art. 16)**
- **Dreptul la ștergere („dreptul de a fi uitat”) (art. 17)**
- **Dreptul la restricționarea prelucrării (art. 18)**
- **Dreptul la portabilitatea datelor (art. 20)**
- **Dreptul la opoziție (art. 21): persoana vizată se poate opune, din motive legate de situația sa particulară, prelucrărilor întemeiate pe interesul legitim, inclusiv CCTV, controlul accesului și verificarea identității; opoziția la marketingul direct este necondiționată și se admite întotdeauna**
- **Dreptul de a depune plângere la ANSPDCP (art. 77)**

Solicitările se pot transmite la privacy@ladepozit.ro.
Operatorul răspunde fără întârzieri nejustificate și în cel mult o lună de la primirea cererii. Dacă este necesar, ținând seama de complexitatea și numărul cererilor, termenul poate fi prelungit cu încă două luni; persoana vizată este informată despre prelungire și motivele întârzierii în prima lună de la primirea cererii.

Persoanele vizate pot solicita, în scop de transparență, accesul la un rezumat al evaluărilor DPIA și LIA, în măsura în care acestea nu conțin informații confidențiale.

Cererile privind imaginile CCTV se analizează potrivit dreptului exercitat, conform secțiunii CCTV. Dreptul de acces include o copie a datelor personale, cu protejarea datelor terților.

Dacă persoana vizată este nemulțumită de răspuns, se poate adresa Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (www.dataprotection.ro) sau instanțelor de judecată competente.

11. Consimțământul pentru profilare și comunicare comercială personalizată

Marketingul direct (newslettere, comunicări promoționale), profilarea și comunicările comerciale personalizate se bazează pe un consimțământ separat, specific, informat și facultativ pentru scopurile și atributele indicate.
Refuzul sau retragerea nu afectează contractul. Consimțământul poate fi retras oricând la privacy@ladepozit.ro, fără a afecta legalitatea prelucrării anterioare retragerii.

12. Transferuri de date și procesatori

La data prezentei versiuni, prelucrările se realizează pe teritoriul Spațiului Economic European și nu se efectuează transferuri în afara SEE. Orice transfer în afara SEE se efectuează numai cu respectarea capitolului V GDPR, în baza unei decizii de adecvare sau a unor garanții adecvate, inclusiv clauze contractuale standard și măsuri suplimentare, după caz. Informațiile privind garanțiile și obținerea unei copii sunt disponibile la privacy@ladepozit.ro.

Datele pot fi comunicate furnizorilor IT, serviciilor de plată, mentenanță CCTV, contabilitate și servicii juridice, numai în limitele scopurilor aplicabile. Rolul fiecărui destinatar se stabilește potrivit activității efective; contractele conform art. 28 GDPR se încheie cu persoanele împuternicite. Calitatea de DPO extern nu determină automat un asemenea rol.

13. Securitatea datelor

Operatorul stabilește măsuri tehnice și organizatorice proporționale cu riscurile și verifică implementarea lor:

- datele se transmit prin conexiuni securizate (TLS) și se stochează în medii protejate, cu acces limitat pe roluri; criptarea la stocare a copiilor CI în DMS și în backupurile aferente este planificată pentru 31 octombrie 2026; măsurile tehnice și organizatorice sunt evaluate și actualizate în raport cu riscurile prelucrării, conform art. 32 GDPR;

- autentificare multifactorială (MFA) și acces pe roluri, cu verificarea configurației și a persoanelor autorizate;
- backup și jurnalizarea accesului, cu testarea restaurării și a ștergerilor;
- program de audit anual DPO și audit IT extern la 24 de luni, cu documentarea realizării;
- procedură de evaluare și notificare a breșelor către ANSPDCP fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore de la luarea la cunoștință, când sunt îndeplinite condițiile art. 33 GDPR;
- program anual de instruire GDPR pentru personalul care prelucrează date.

14. Exercitarea drepturilor și procedura internă

Procedura internă de gestionare a solicitărilor GDPR prevede:

- identificarea solicitantului prin mijloace proporționale;
- înregistrarea cererii și răspuns în termenul legal;
- analizarea individuală a cererilor CCTV, inclusiv ștergere, restricționare și acces, conform condițiilor legale;
- ștergerea datelor la termenele din prezenta politică, de regulă automat și, atunci când automatizarea nu este posibilă, manual;
- păstrarea evidenței cererilor timp de 3 ani de la soluționare, cu prelungire numai pentru un litigiu sau o obligație legală documentată.

15. Notă de confidențialitate

Acest document este destinat informării clienților, colaboratorilor și persoanelor vizate. Orice modificare semnificativă a modului de prelucrare a datelor va fi publicată pe www.ladepozit.ro și comunicată, dacă este cazul, clienților activi prin e-mail. Prezenta politică va fi revizuită anual sau ori de câte ori intervin modificări tehnologice, legale sau operaționale care afectează procesele de prelucrare, inclusiv implementarea criptării la nivel de infrastructură.

PRIVACY POLICY (GDPR POLICY)

OSIRIS INVESTMENT S.R.L. / LaDepozit

Version: 3.1 | Revision: September 2026

1. Introduction

As of May 25, 2018, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR") applies, establishing the legal framework for the processing of personal data within the European Union.

Osiris Investment S.R.L., a Romanian legal entity registered with the Trade Registry under no. J40/8391/2019, with its registered office in Bucharest, Str. Cristian Tell no. 19, room 2, 1st floor, ap. 5bis, District 1, having VAT number RO 41318860 ("the **Controller**" or "**LaDepozit**"), complies with the provisions of the GDPR and Law no. 190/2018 and applies appropriate technical and organizational measures to protect personal data.

The Controller owns the registered trademark LaDepozit and performs activities involving the provision of secured self-storage units and the administration of the related digital platform.

2. Contact details

General e-mail: contact@ladepozit.ro
Data Protection Officer ("**DPO**"): Buda Și Asociații S.P.A.R.L. (Buda Partners), represented by Attorney Ștefan Ionuț Buda
E-mail: privacy@ladepozit.ro

3. Purposes and lawful bases of processing

LaDepozit collects and processes personal data for the following purposes:

Purpose of processing	Lawful basis (Art. 6 GDPR)	Examples of activities
Contract conclusion and execution	Art. 6(1)(b)	Account creation, unit reservation, electronic signing, invoicing
Compliance with legal obligations	Art. 6(1)(c)	Accounting reports and tax archiving under applicable statutory obligations
Safety and security of persons and goods	Art. 6(1)(f)	Video surveillance (CCTV), electronic access control
Client identity verification and fraud prevention	Art. 6(1)(f)	Identity verification and retention of ID copies within the documented necessity
Administrative communications and customer support	Art. 6(1)(b) and (f)	Notifications, commercial correspondence, responses to inquiries

Purpose of processing	Lawful basis (Art. 6 GDPR)	Examples of activities
Direct marketing (optional)	Art. 6(1)(a)	Newsletters, promotional communications based on consent
Internal profiling and personalized commercial communication (optional)	Art. 6(1)(a) – explicit consent	Internal analysis of customer behavior, demographic segmentation, and personalized offers sent only to individuals who have explicitly granted consent. The absence of consent does not affect the ability to conclude the rental contract.
Access control and identity verification of representatives designated by corporate clients	Art. 6(1)(f) – legitimate interest	Verifying the identity of persons designated by the corporate client to act on its behalf; access control in the storage facilities; prevention of unauthorized access
Access control and identity verification of actual users of the storage units	Art. 6(1)(f) – legitimate interest	Verifying the identity of persons delegated or authorized by the client to actually use the storage unit; fraud prevention; security of stored goods and premises

Note on legitimate interest: The processing of personal data of representatives of corporate clients and of actual users of the storage units on the basis of legitimate interest (Art. 6(1)(f) GDPR) relies on the objective necessity to control access to secured premises containing third-party goods, to prevent unauthorized access and fraud, and to protect the legitimate interests of the Controller and of the other clients. The Controller has carried out a documented Legitimate Interest Assessment (LIA), available upon request at privacy@ladepozit.ro. The Controller's legitimate interest does not override the fundamental rights and freedoms of the data subjects, the processing being limited to the data strictly necessary for the declared purpose.

The Controller does not seek to collect special categories of data. Any sensitive data incidentally captured by CCTV are appropriately protected. Internal profiling for segmentation and personalised commercial communications may use only attributes covered by separate, specific, informed and optional consent. The CNP identifier and the ID image are not used for these purposes; any derived attributes (age, gender, locality) are kept separate from the ID copy. No decisions based solely on automated processing producing legal or similarly significant effects are taken within Article 22 GDPR. Before enabling profiling, the Controller documents the data flow, data, retention, consent and risks and updates the DPIA.

4. Categories of processed data

- Identification data: name, surname, personal identification number (CNP), ID series and number, ID copy (securely stored), signature. Identification and contact data are required for concluding the contract and granting access to the locations; without them,

the contract cannot be concluded or access cannot be granted. Data for marketing and profiling are optional.

- Contact data: e-mail, phone number, address.
- Contractual and payment data: IBAN, invoices, payment history, accounting documents.
- Technical data: IP addresses, session identifiers, platform access logs, PIN codes/access cards.
- Video images: CCTV recordings from common areas and LaDepozit perimeters.

5. Video surveillance (CCTV)

LaDepozit uses CCTV systems exclusively to ensure the safety of persons and goods and to prevent theft or vandalism.

Cameras are installed only in access areas and common spaces, with no equipment inside storage units.

CCTV footage is retained for up to 30 days and erased by overwriting, except for separate, justified preservation for incidents, disputes or requests under the rules below.

Access to recordings is limited to designated authorised personnel and, where necessary for their duties, the DPO, in justified and logged cases. Requests concerning CCTV footage are assessed individually according to the right exercised. Where Article 17 GDPR applies and no statutory exception is available, footage is erased without undue delay, including by irreversible anonymisation where appropriate. Restriction applies under Article 18 GDPR and does not automatically replace erasure. Technical limitations are documented and remedied; they do not, by themselves, justify refusal or postponement until automatic overwriting. Footage necessary to fulfil an access request or deal with a dispute is preserved separately, with restricted access, only for the justified period.

Data subjects are informed through visible signage at facility entrances and this policy, in accordance with EDPB Guidelines 3/2019[1].

6. Processing of data of representatives of corporate clients and of actual users of the storage units

The Controller processes personal data of the following categories of persons who are not a direct contractual party, in the context of access control and security activities:

- **Category 2 – Representatives / contact persons of corporate clients:** natural persons designated by a corporate client to act on its behalf in the relationship with LaDepozit (legal representatives, agents, contact persons).

[1] on processing personal data through video devices (version 2.0, adopted on 29 January 2020)

- **Category 3 – Actual users of the storage units:** natural persons delegated or authorized by a client (natural or legal person) to actually use the storage unit, including employees, collaborators, representatives or other persons designated by the client.

The processing of data of persons in Categories 2 and 3 is based on the Controller's legitimate interest in access control, identity verification, fraud prevention and the protection of persons and property. Persons in Categories 2 and 3 are informed through this Privacy Policy, available at https://ladepozit.ro/politica-gdpr/. Where data are obtained directly from the data subject, the policy is made available at the time of collection. Where data are obtained from the client, the policy is communicated within a reasonable period, no later than one month after obtaining the data, and at the latest at the first communication with the data subject or the first disclosure to another recipient, whichever occurs earlier. The link is included in the data collection screen and in the e-mail/SMS containing access credentials, without postponing any earlier information obligation. The Controller retains evidence of communication and of the policy version provided. The designating client is additionally contractually required to provide the policy before communicating the person's data to LaDepozit; this does not replace the Controller's responsibility. No separate notices or acknowledgments of receipt are required for these categories.

For Categories 2 and 3, the ID copy and CNP are processed under Article 6(1)(f) GDPR only to the extent that their necessity for access control and fraud prevention is demonstrated. The CNP may provide stable linkage between records of the same person designated by several clients or presenting a replacement identity document. The Controller documents why identity verification without retaining a copy, an internal identifier, or the ID series and number do not sufficiently achieve the specific purpose. Administrative convenience or contact-person status without physical access does not, by itself, justify collecting an ID copy and CNP.

7. Processing of third-party data within LaDepozit premises

In the course of its operations, the Controller may process personal data of individuals who do not have a direct contractual relationship with it ("third parties"), such as persons accompanying clients, visitors, supplier representatives, or others occasionally present on LaDepozit premises.

Such data are mainly processed through CCTV systems or access and security control mechanisms. Processing is based on the Controller's legitimate interest (Art. 6(1)(f) GDPR) – ensuring safety, protecting persons and property, and preventing incidents. Access to monitored or restricted areas implies acknowledgment of video surveillance and its purpose, as displayed through visible information notices.

8. Storage of ID copies

LaDepozit requests and retains ID copies only to the extent necessary and documented for identity verification, access control and fraud prevention for the categories described above.

Contact-person status without physical access does not, by itself, justify collecting an ID copy or CNP.

ID copies are collected through secure channels (TLS upload or controlled scanning) and stored in the internal document management system (DMS).

Data are transmitted through secure connections (TLS) and stored in protected environments with role-based access restrictions; encryption at rest of ID copies in the DMS and the associated backups is planned for 31 October 2026. Technical and organisational measures are assessed and updated in light of processing risks, under Article 32 GDPR. Access is limited to named authorised staff within Sales and Contracting; DPO access is limited to justified cases and what is necessary for their duties.

ID copies of individual clients are retained for the contract duration; subsequent retention, for no more than 5 years after termination, is allowed only where the need to establish, exercise or defend legal claims is documented and periodically reviewed. ID copies and CNPs of representatives, contact persons and designated users are retained only for the duration of their designation or access entitlement and are deleted when it ends, except for data strictly necessary for a specific incident, dispute or legal obligation, retained separately for the justified period. Contractual and accounting records follow their own statutory retention periods, which do not automatically extend to ID copies. Residual backup copies are removed within 30 days after deletion from active systems, are not used for ordinary processing, and deletions are reapplied upon restoration. The CNP of individual clients, included in the contractual documents, follows their retention period (5 years after contract termination); marketing and profiling data are kept until consent is withdrawn or for a maximum of 2 years after the last interaction. Unauthorised copying, printing or sending ID copies through e-mail/WhatsApp is prohibited; disclosures required for data subject rights use secure channels.

9. Retention periods and deletion mechanisms

Type of data	Maximum retention period	Deletion mechanism
Contractual documents	5 years after contract termination, subject to applicable special statutory periods	Automatic deletion / anonymization
Contact and correspondence data	2 years after end of relationship	Automatic CRM deletion
IT logs and electronic access data	12 months	Automatic log rotation
CCTV recordings	Up to 30 days; separate preservation only in justified cases described in the CCTV section	Automatic overwrite
ID copies	Separate periods for clients and designated persons	Deletion from the DMS when the retention period expires,

	under “Storage of ID copies”; removal from backups within 30 days after deletion from active systems	normally automatically and, where automation is not possible, manually by authorised personnel.

The Controller periodically verifies compliance with retention periods. Deletion is normally performed automatically and, where automation is not possible, manually by authorised personnel, without extending the applicable retention periods.

10. Data subjects’ rights

Data subjects have the following rights under the GDPR:

- **Right to information (Art. 13–14)**
- **Right of access (Art. 15)**
- **Right to rectification (Art. 16)**
- **Right to erasure (“right to be forgotten”) (Art. 17)**
- **Right to restriction of processing (Art. 18)**
- **Right to data portability (Art. 20) ● Right to object (Art. 21): the data subject may object, on grounds relating to their particular situation, to processing based on legitimate interest, including CCTV, access control and identity verification; objection to direct marketing is unconditional and is always granted**
- **Right to lodge a complaint with the National Supervisory Authority for Personal Data Processing (ANSPDCP) (Art. 77)**

Requests may be sent to privacy@ladepozit.ro.

The Controller responds without undue delay and no later than one month after receiving the request. Where necessary, taking account of the complexity and number of requests, this period may be extended by two further months; the data subject is informed of the extension and the reasons for the delay within the first month.

Data subjects may request access to a summary of DPIA and LIA evaluations, insofar as they do not contain confidential information.

Requests concerning CCTV footage are assessed according to the right exercised, as described in the CCTV section. The right of access includes a copy of personal data, while protecting third-party data.

If a data subject is dissatisfied with the response, they may lodge a complaint with ANSPDCP (www.dataprotection.ro) or competent courts of law.

11. Consent for profiling and personalized commercial communication

Direct marketing (newsletters, promotional communications), profiling and personalised commercial communications require separate, specific, informed and optional consent for the

stated purposes and attributes. Refusal or withdrawal does not affect the contract. Consent may be withdrawn at any time at privacy@ladepozit.ro without affecting the lawfulness of processing before withdrawal.

12. Data transfers and processors

As at the date of this version, processing takes place within the European Economic Area and no transfers outside the EEA are carried out. Any transfer outside the EEA must comply with Chapter V GDPR, based on an adequacy decision or appropriate safeguards, including standard contractual clauses and supplementary measures where applicable. Information on safeguards and obtaining a copy is available at privacy@ladepozit.ro. Data may be disclosed to IT, payment, CCTV maintenance, accounting and legal service providers only within the applicable purposes. Each recipient's role is determined by its actual activities; Article 28 GDPR agreements are concluded with processors. External DPO status does not automatically establish such a role.

13. Data Security

The Controller establishes technical and organisational measures proportionate to the risks and verifies their implementation:

- Data are transmitted through secure connections (TLS) and stored in protected environments with role-based access restrictions; encryption at rest of ID copies in the DMS and the associated backups is planned for 31 October 2026. Technical and organisational measures are assessed and updated in light of processing risks, under Article 32 GDPR.
- Multi-factor authentication (MFA) and role-based access, with verification of configuration and authorised users.
- Backups and access logging, with testing of restoration and deletions.
- An annual DPO audit programme and external IT audit every 24 months, with completion documented.
- A procedure for assessing breaches and notifying ANSPDCP without undue delay and, where feasible, within 72 hours of awareness, where Article 33 GDPR requires notification.
- An annual GDPR training programme for staff processing personal data.

14. Exercising rights and internal procedure

The Internal Procedure for Managing Data Subject Requests provides for:

- verifying the identity of the requester through proportional means;
- registering the request and providing confirmation of receipt;
- analyzing the request and issuing a response within the legal timeframe;

- individual assessment of CCTV requests, including erasure, restriction and access under the applicable legal conditions;
- deletion of data within the retention periods specified in this policy, normally automatically and, where automation is not possible, manually;
- retention of request records for 3 years after resolution, with extensions only for a documented dispute or statutory obligation.

15. Confidentiality notice

This document is intended to inform clients, partners, and data subjects. Any significant change in the data processing practices will be published on www.ladepozit.ro and communicated, where applicable, to active clients via e-mail. This policy will be reviewed annually or whenever technological, legal, or operational changes occur that impact processing activities, including the implementation of infrastructure-level encryption.