



AUTORITATEA  
PENTRU  
DIGITALIZAREA  
ROMÂNIEI

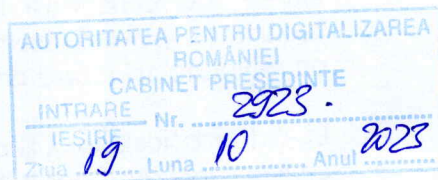
BIROUL COMUNICARE PUBLICĂ

Nr.2487/ 21-L544/18.10.2023

Către:

Domnul Adrian Vasilache - jurnalist HotNews

E-mail: [adrian.vasilache@hotnews.ro](mailto:adrian.vasilache@hotnews.ro)



Ca urmare a solicitării dumneavoastră, formulată în baza Legii 544/2001, înregistrată la Autoritatea pentru Digitalizarea României cu nr. 2487/17.10.2023 și în registrul special al Legii nr. 544/2001 cu nr. 21/L544/17.10.2023, vă comunicăm următoarele:

RoelD este o platformă centralizată care asigură identificarea și autentificarea unică pentru cetățeni în ideea accesării de servicii publice puse la dispoziție de către organismele din sectorul public, servicii furnizate de către platforme interconectate cu aceasta.

Astfel utilizarea platformei RoelD simplifică accesul la serviciile publice și contribuie la creșterea gradului de utilizare. Toate acestea conduc la accelerarea digitalizării proceselor și la îmbunătățirea interacțiunii cetățeanului cu instituțiile statului.

De asemenea, platforma vine în sprijinul instituțiilor astfel încât nu mai este nevoie ca fiecare să își dezvolte, auditeze și administreze platforme de identificare la distanță prin mijloace video, ceea ce implică numeroase costuri suplimentare, dar aduce și un plus în dezvoltarea, cunoașterea și utilizarea serviciilor publice, deoarece sunt mult mai ușor de accesat (după obținerea identității electronice este suficientă o singură autentificare pentru a folosi mai multe servicii).

Platforma RoelD este singura platformă de identificare la distanță prin mijloace video interconectată la DPABD, fapt ce contribuie la creșterea gradului de securitate privind furnizarea serviciilor de identificare la distanță. Pentru a putea fi utilizate serviciile de identificare prin mijloace video este necesar ca acestea să fie recunoscute și reglementate la nivel național, conform prevederilor art. 24 lit. d), din Regulamentul (UE) 910/2014.

În prezent, Normele privind reglementarea, recunoașterea, aprobarea sau acceptarea procedurii de identificare a persoanei la distanță utilizând mijloace video intrate în vigoare prin Decizia nr. 564/2021 au rol de reglementare națională și reglementează utilizarea mijloacelor video în procesul de identificare în cadrul activităților desfășurate atât de operatorii economici, cât și de către autoritățile și instituțiile publice.



Bd. Libertății, nr. 14  
Sector 5 | București



[contact@adr.gov.ro](mailto:contact@adr.gov.ro)



[www.adr.gov.ro](http://www.adr.gov.ro)  
[fb.com/digitalizareaRomaniei](https://fb.com/digitalizareaRomaniei)



+40 374 541 179



Platforma RoelD este singura platformă de identificare la distanță prin mijloace video, interconectată la DPABD, fapt ce contribuie la creșterea gradului de securitate privind furnizarea serviciilor de identificare la distanță și oferă un nivel de asigurare echivalent din perspectiva fiabilității cu prezența fizică.

LL-C (Certification) Czech Republic a.s. (organism de evaluare a conformității în concordanță cu prevederile Regulamentului UE 910) a evaluat conformitatea soluției tehnice și a procedurii de identificare video a persoanei la distanță din cadrul platformei RoelD ținând cont de:

- a) Normele ADR privind reglementarea, recunoașterea, aprobarea sau acceptarea procedurii de identificare a persoanei la distanță utilizând mijloace video intrate în vigoare prin Decizia 564/2021;
- b) Regulamentul UE nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă, al standardului ISO/IEC 17065;
- c) Standardul ETSI TS 119 461 (Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects).

În urma analizării s-a întocmit un raport de evaluare a conformității care specifică faptul că platforma respectă cerințele normelor.

Normele ADR privind reglementarea, recunoașterea, aprobarea sau acceptarea procedurii de identificare a persoanei la distanță utilizând mijloace video:

- reglementează cadrul general privind utilizarea mijloacelor video pentru identificarea persoanei la distanță;
- stabilește obligațiile și responsabilitățile pentru entitățile care participă la procedura de identificare a persoanei la distanță prin mijloace video;
- stabilesc cerințele tehnice privind procedura de identificare a persoanei la distanță prin mijloace video etc.
- stabilesc cerințe privind prelucrarea datelor cu caracter personal. (ex. Art. 12 și 22)

Art. 12 /Norme

Furnizorii de servicii de identificare sunt obligați să respecte toate dispozițiile legale cu privire la protecția datelor cu caracter personal prevăzute în Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE și în Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), cu modificările ulterioare.

Art. 22 /Norme





- (1) Întregul proces de identificare a persoanei la distanță utilizând mijloace video, în toate etapele sale, trebuie să fie înregistrat și păstrat.
- (2) Toate înregistrările audio-video, datele și informațiile aferente procesului de identificare a persoanei la distanță utilizând mijloace video vor fi păstrate într-o formă admisă în procedurile judiciare.
- (3) Punerea la dispoziția autorităților competente a informațiilor obținute prin procesul de identificare a persoanei la distanță utilizând mijloace video se face cu respectarea prevederilor Legii nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date.

La verificarea conformității cu normele s-au avut în vedere și prevederile normelor privind prelucrarea datelor cu caracter personal.

Referitor la evaluarea DPIA, ADR în calitate de operator/procesator de date este obligat să evalueze impactul potențial asupra drepturilor și libertăților persoanelor pe care l-ar putea aduce un incident de securitate (legat de sistemul de prelucrare a datelor). Incidentul de securitate poate fi asociat cu orice tip de încălcare a confidențialității, integrității sau disponibilității datelor cu caracter personal.

Datorită naturii ad-hoc și diversității operațiunilor de prelucrare a datelor cu caracter personal, poate fi utilizată doar o abordare calitativă, bazată pe înțelegerea generală (de către organizație) a operațiunii sale specifice de prelucrare a datelor. În acest scop, evaluarea impactului se bazează pe o serie de parametri, precum tipul și volumul datelor cu caracter personal, criticitatea operațiunii de prelucrare, caracteristicile speciale ale operatorului/operatorului de date, caracteristicile speciale ale persoanelor vizate, precum și nivelul de identificare a persoanelor vizate. În urma acestei evaluări, controlorului i se cere să evalueze impactul, pe baza a patru niveluri predefinite, adică scăzut, mediu, ridicat și foarte ridicat.

O amenințare este orice circumstanță sau eveniment care are potențialul de a afecta negativ securitatea datelor cu caracter personal. În acest caz, intenția ADR este să înțeleagă amenințările legate de mediul general al prelucrării datelor cu caracter personal (extern sau intern) și să evalueze probabilitatea acestora (probabilitatea apariției amenințărilor). În acest sens, ar putea fi luate în considerare diferite niveluri și tipuri de amenințări la adresa confidențialității, integrității și disponibilității datelor cu caracter personal.

Având în vedere cele de mai sus, sistemul tratează situațiile într-o clasă de risc ridicat, iar măsurile sunt cele stabilite de bunele practici europene.





Sunt luate în considerare două mari categorii de măsuri, organizatorice și tehnice, care sunt împărțite în continuare în categorii specifice. În principiu, acestea urmează clasificarea dată în ISO/IEC 27001 Anexa A și ISO/IEC 27002.

Analiza de risc este o obligație a Regulamentului 910/2014 - Articolul 19 prevede că furnizorii de servicii de încredere calificați și necalificați trebuie să ia măsuri tehnice și organizatorice adecvate pentru a gestiona riscurile prezentate pentru securitatea serviciilor de încredere pe care le furnizează. Acest lucru necesită ca ADR să efectueze o evaluare a riscurilor pentru a se asigura că nivelul de securitate este proporțional cu gradul de risc și pentru a minimiza impactul incidentelor de securitate. ADR a demarat un proces pentru alinierea la standardele ISO 27.000.

Multe standarde oferă deja linii directoare pentru managementul riscurilor. Unul dintre ele este [ISO/IEC 27005]. Acesta oferă linii directoare pentru managementul riscului de securitate a informațiilor într-o organizație, susținând în special cerințele unui sistem de management al securității informațiilor (ISMS) conform [ISO/IEC 27001].

ADR a utilizat metodologia ENISA (REMOTE ID PROOFING March 2021) care prezintă orientări specifice și practice cu privire la gestionarea riscurilor de securitate pentru metodele de verificare a identității, bazate în principal pe cerințele [ISO/IEC 27005] și pe procesul de management al riscurilor prezentat în [ENISA].

S-au respectat standardele de bună practică a LOA pentru un nivel de încredere ridicat așa cum sunt descrise în Regulamentul de punere în aplicare (UE) 2015/1502.

<https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32015R1502>

Între alte elemente, cerințele pentru infrastructură și personal sunt similare pentru orice nivel de asigurare a încrederii:

- Existența unor proceduri care să garanteze că personalul și subcontractanții sunt suficient de bine formați, calificați și experimentați în ceea ce privește abilitățile necesare pentru a îndeplini rolurile care le revin.
- Existența unui număr suficient de angajați și de subcontractanți pentru a funcționa în mod adecvat și a asigura resurse serviciului în conformitate cu politicile și procedurile sale.
- Infrastructura utilizată pentru prestarea serviciilor este monitorizată continuu și protejată împotriva pagubelor provocate de evenimente de mediu, a accesului neautorizat și a altor factori care pot influența securitatea serviciului.
- Prin infrastructura utilizată pentru prestarea serviciului se asigură că accesul la zonele unde se păstrează sau se prelucrează informații personale, criptografice sau alte informații sensibile este limitat la personalul autorizat sau la subcontractanți.





În cadrul procesului de analiză a riscurilor vă precizăm că, în conformitate cu Regulamentul (UE)2015/1502, în vederea respectării unui sistem de management al securității informațiilor, au fost luate măsuri pentru a reduce la minimum riscul ca identitatea persoanei să nu fie cea pretinsă, luând în considerare, de exemplu, riscul utilizării unor dovezi pierdute, furate, suspendate, revocate sau expirate.

Astfel măsurile analizate s-au bazat pe factorul de autentificare inerent, care presupune un factor de autentificare care se bazează pe o caracteristică fizică a unei persoane fizice și în cazul căruia subiectul trebuie să demonstreze că prezintă respectiva caracteristică fizică.

Un alt factor analizat l-a constituit minimizarea riscului de modificare a datelor de identificare personală, fapt ce a necesitat cerința de asigurare cu privire la dovedirea și verificarea identității.

Referitor la întrebarea privind numărul de persoane care și-au făcut cont menționăm faptul că până în acest moment au fost create 16.000 de conturi în sistemul ROeID.

Referitor la întrebarea privind garanțiile de securitate oferite pentru datele personale colectate vă comunicăm că securitatea platformei este asigurată de echipamentele de securitate cibernetică achiziționate în cadrul proiectului.

Referitor la întrebarea privind utilitatea ROeID, pentru a înțelege care sunt obiectivele sistemului vă invităm la sediul ADR pentru o prezentare a întregii platforme.

Datele de contact ale ADR se regăsesc la adresa <https://www.adr.gov.ro/contact/>. În vederea stabilirii unei întâlniri vă rugăm să ne contactați la adresa de [contact@adr.gov.ro](mailto:contact@adr.gov.ro) sau tel. 0374541179, persoană de contact pentru solicitările conform Legii nr. 544/2001 Gabriela Popescu

Cu aleasă considerație,

**Dragoș-Cristian VLAD**  
Președinte



The first part of the document discusses the importance of maintaining accurate records of all transactions. It emphasizes that every entry should be supported by a valid receipt or invoice to ensure transparency and accountability.

In addition, it is crucial to review the records regularly to identify any discrepancies or errors. This proactive approach helps in resolving issues before they escalate and ensures that the financial data remains reliable.

The second section outlines the specific steps for recording transactions. It includes instructions on how to categorize expenses, record income, and maintain a clear audit trail for each entry.

Furthermore, the document provides guidelines on how to handle complex transactions, such as those involving multiple parties or currencies. It stresses the need for clear communication and documentation in these cases.

Finally, the document concludes by reiterating the importance of consistency and accuracy in record-keeping. It encourages users to adhere to the provided guidelines to ensure the integrity of their financial records.