Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Moldova

COUNTRY Moldova

INDUSTRY Government & Public Services

LAST UPDATED 5 November 2026

KEY REGULATORS Information and Security Service · E-Government Agency · Public Services Agency

Key takeaways

- Moldova's state digital identity rests on qualified electronic signatures (legally equal to a handwritten signature) carried on the new chip identity card, on a mobile SIM, or on a USB token, plus the state login (MPass) and signing (MSign) services.
- Any document a private company or individual signs electronically in dealings with a public authority needs a qualified electronic signature; a lower-grade "advanced" signature is not accepted there.
- A provider that wants to identify people fully online for a qualified certificate must hold qualified trust service provider status from the Information and Security Service and notify it 30 days before using the remote method.
- Remote identification must combine a face match against the identity document chip or the State Population Register with certified liveness detection; fully automated checks accept only identity cards and passports whose chip can be read by NFC (near-field communication).
- The technical rules for low, substantial and high assurance levels are still a draft, and a Government bill to replace the e-ID law with an EU-aligned one (including a certified digital identity wallet) entered Parliament on 28 October 2026. Build to the current law and expect changes.

The market for digital identity and public e-services is open to private firms, but on the state's terms. Private companies can connect to MPass and MSign under a paid contract with the E-Government Agency, and can become qualified trust service providers after a conformity assessment and a decision by the Information and Security Service (SIS), which supervises electronic identification and trust services.

The principal authorities are SIS (supervisor), the E-Government Agency (owner of MPass, MSign and the EVO app), the Information Technology and Cyber Security Service (the state issuer of qualified signatures) and the Public Services Agency (identity documents and the State Population Register). The biggest obstacle for a new entrant is the qualified status itself: online identification for qualified certificates is reserved to providers that hold it, and the Government's remote identification procedure must be notified to SIS before use.

CONTENTS

1 Who regulates this sector
2 Licensing and authorisation
3 Identity framework (AML rules do not apply)
4 Identity verification and onboarding
5 Digital channels: what's different
6 Data protection and biometrics
7 Sector-specific obligations
8 Risk indicators and red flags
9 Enforcement and penalties
10 Recent changes and what to watch
11 What this means for identity verification
▪ Sources

1 Who regulates this sector

Authority	Remit	Level	Official site
Information and Security Service (SIS)	Supervisory body for electronic identification and trust services; grants qualified status; keeps the register of qualified providers and the Trusted List	National	sis.md
E-Government Agency (AGE)	Owner of MPass (authentication), MSign (signing) and the EVO app and wallet; contracts with private users	National	egov.md
Information Technology and Cyber Security Service (STISC)	Technical administrator of MPass; manages the Government public key infrastructure and issues qualified electronic signatures	National	stisc.gov.md
Public Services Agency (ASP)	Identity documents for citizens; holds the State Population Register	National	asp.gov.md
Ministry of Economic Development and Digitalization (MDED)	Policy owner and author of the 2026 draft e-ID rules	National	mded.gov.md
National Center for Personal Data Protection (CNPDCP)	Data protection supervisor, including biometric processing	National	datepersonale.md

Office for Prevention and Fight against Money Laundering (SPCSB)	Financial intelligence unit; receives reports from public authorities	National	spcsb.md

2 Licensing and authorisation

Qualified trust service provider status

Under Law No. 124 of 19 May 2022 on electronic identification and trust services (last amended by Law 227/2025, in force 30 December 2025) `In force`, providers may be qualified or non-qualified (art. 6). A non-qualified provider that wants to offer qualified services sends SIS a notification with a conformity assessment report from a conformity assessment body (art. 8(2)). SIS checks compliance, grants the status and publishes the provider on the Trusted List; the provider counts as qualified from the day it is listed (art. 8(4)-(5)). Qualified providers keep all relevant records for 15 years and commission a conformity audit at least every two years (art. 10(2), points 9-10). The SIS register lists STISC and four EU-based providers.

Remote identification methods

Government Decision No. 977 of 6 December 2023 (published 18 January 2024) `In force` sets two alternative remote identification methods for natural persons: automated digital verification without a human operator, and digital verification with a human operator. Using them is optional for qualified providers (point 2) and needs no prior authorisation (Procedure, point 4), but the provider must notify SIS 30 days before starting (point 5). The notification includes the system description, identification policy, a software conformity report and liveness certification (point 6), from an accredited assessment body with at least five years' biometric experience (point 7).

Connecting to state platforms

Public authorities integrate MPass and MSign free of charge. Natural persons and private legal entities that own information systems may sign a paid contract with the E-Government Agency to use MPass authentication (Government Decision No. 1090 of 31 December 2013, point 4^2, last amended 28 February 2025) and MSign signing (Government Decision No. 405 of 2 June 2014, point 5^1, last amended 8 June 2024).

3 Identity framework (AML rules do not apply)

Public authorities are not reporting entities under Law No. 308 of 22 December 2017 on preventing and combating money laundering and terrorist financing (last amended by Law No. 146/2026, in force 13 August 2026), whose art. 4(1) lists financial firms, gambling organisers and professionals. Customer due diligence and threshold reporting therefore do not apply to public services.

Two narrower duties do apply. Public authorities other than AML supervisors must report possible breaches of the law that they identify in their work to SPCSB immediately and no later than 5 working days (art. 4(4)). The Public Services Agency must report suspicious activities or transactions identified while delivering public services within 24 hours (art. 4(6)).

Identity in public services rests instead on Law 124/2022, Government Decision 977/2023, Law No. 273 of 9 November 1994 on identity documents (republished 18 December 2025) and Law No. 142 of 19 July 2018 on data exchange and interoperability.

Electronic identification means can have three assurance levels: low, substantial and high (Law 124/2022, art. 5^1(1), inserted by Law No. 117 of 29 May 2025 and applicable six months after its publication on 18 June 2025). The Government sets the criteria, conformity assessment bodies check them, and SIS publishes the list of e-ID means and their levels on its website (art. 5^1(2)-(4)). As of November 2026 the Government decision setting those criteria remains a draft (section 10).

4 Identity verification and onboarding

The national identity documents

The identity card proves identity and Moldovan citizenship (Law 273/1994, art. 3(1)). Its electronic storage medium holds the printed data, a qualified certificate for electronic signature, and biometric data: the facial image and fingerprints (art. 3(6)); the law prescribes the same chip contents for residence cards, issued to foreign nationals by the General Inspectorate for Migration (art. 4(1^1)). A citizen who can identify electronically may generate a digital version of the card in the EVO app (art. 4(6)), which has the same legal force as the physical card and draws its data from the State Population Register (Government Decision No. 125 of 18 February 2013, Annex 1, point 20^1, last amended 2 July 2026).

Identification before issuing a qualified certificate

A qualified provider must verify the identity of the person receiving a qualified certificate, directly or through a third party, in one of four ways (Law 124/2022, art. 10(2), point 4): in person; remotely using an e-ID means issued after the person's physical presence; through an existing qualified certificate, qualified signature or qualified seal; or by other nationally recognised methods offering equivalent assurance to physical presence, set by the Government in Government Decision 977/2023.

The remote procedure

The Procedure approved by Government Decision 977/2023 runs in four stages: collection of identification data, verification, an electronic record file, and transmission of the result to the client service (point 14). It collects name, state identification number (IDNP), document data, face photo and video, and contact details (point 17). The document's authenticity and status (not declared lost or stolen) are checked against external sources, including the State Population Register, and may be verified cryptographically by NFC (point 21).

Identity is confirmed by facial biometric matching and deep-learning liveness detection, comparing a frame from the selfie video with the photo on the document chip or from the State Population Register (point 22). Liveness detection software must be certified to ISO/IEC 30107 presentation attack detection, at least level II (point 13), and the software must follow ISO/IEC 15408, 27034 or 24745 (points 11-12). Only identity cards and passports are accepted; in fully automated mode, only documents whose authenticity can be verified cryptographically by NFC (Annex).

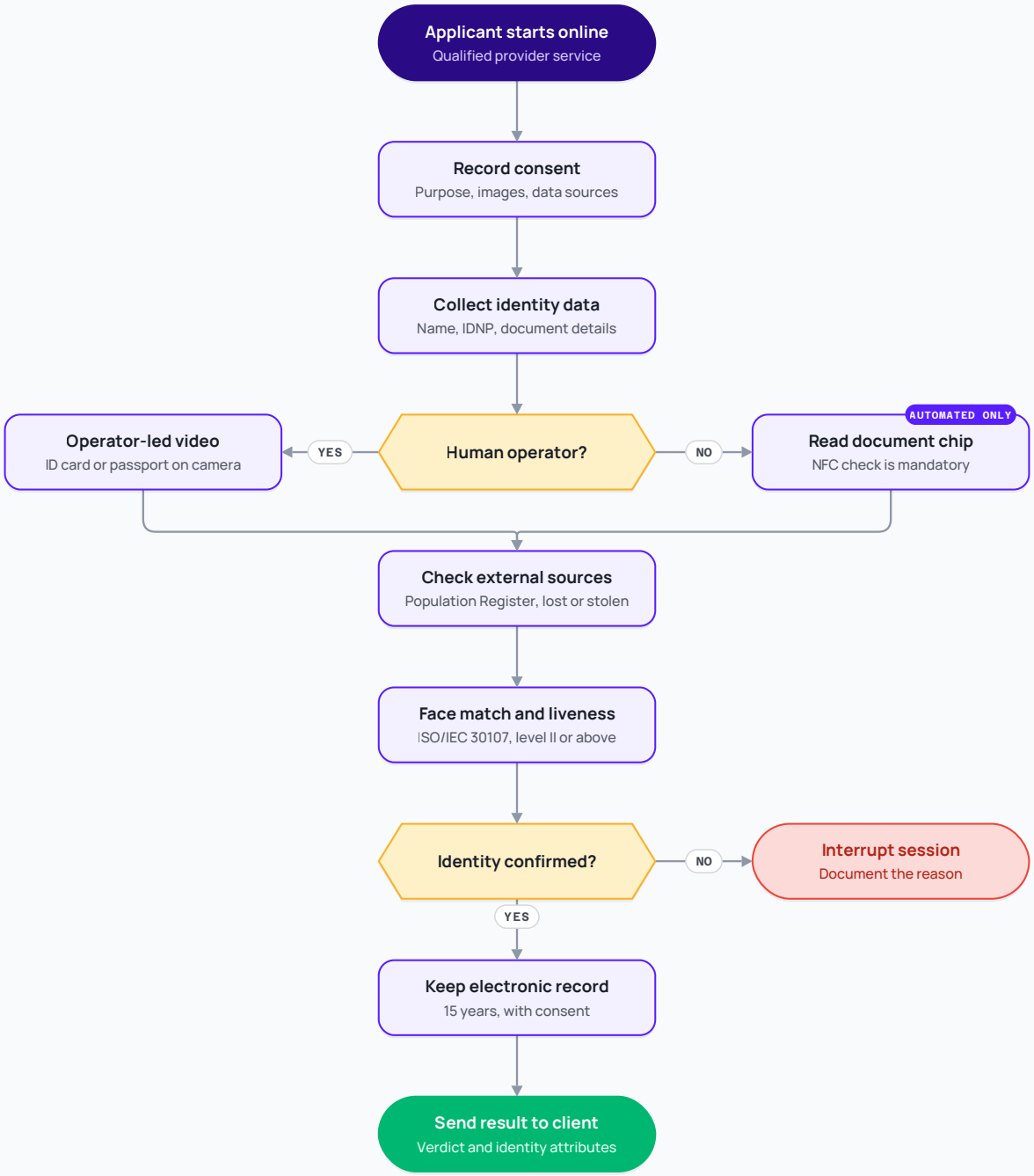


Figure 1. Remote identification of a natural person under Government Decision 977/2023.

5 Digital channels: what's different

Bottom line: the legal value of a qualified signature is the same in every channel, but identifying someone online for a qualified certificate is a separately notified method with prescribed biometrics, document types, session rules and a recorded evidence file.

Requirement	In person	Online / remote	Difference
Identification for a qualified certificate	Physical presence	Prior e-ID, existing qualified signature, or HG 977 method	Differs
Prior notice to SIS	Qualified status only	Notify SIS 30 days before using HG 977 methods (no authorisation)	Differs
Accepted documents	Identity document	Identity card or passport; NFC-readable only if automated	Differs
Biometric check	Not prescribed	Face match plus certified liveness (ISO/IEC 30107, level II)	Differs
Session rules	Not prescribed	Real time, single uninterrupted session; result within 72 hours if an operator reviews	Differs
Evidence kept	Relevant records, 15 years	Record file with consent, images and video, 15 years	Differs
Legal value of a qualified signature	Equal to handwritten	Equal to handwritten	Same
Signature in dealings with public bodies	Qualified (advanced not admitted)	Qualified (advanced not admitted)	Same
Asking citizens for documents	Not where data is on the interoperability platform	Not where data is on the interoperability platform	Same

Automated versus operator-led identification

Fully automated identification must include a random element in prompts and video sequences to defeat pre-recorded sessions, and cross-checks the applicant's data against the machine-readable zone (MRZ) where possible (HG 977/2023, Procedure, point 30). Operator-led sessions need staff trained at least yearly in biometrics, data protection and information security (points 9-10).

Session rules and channel-neutral rules

Identification runs in real time, in one uninterrupted session over an encrypted channel (point 31); poor quality or any doubt about the document stops it (points 32-33). By contrast, a qualified signature equals a handwritten one in every channel (Law 124/2022, art. 21(2), 40(1)), and public bodies may not ask for documents whose data they can get through the interoperability platform (Law 142/2018, art. 6(3[1])).

6 Data protection and biometrics

Law No. 195 of 25 July 2024 on personal data protection `In force since 23 Aug 2026` transposes the EU General Data Protection Regulation and replaces Law 133/2011. Biometric data processed to uniquely identify a person are a special category, processed only under an exception such as explicit consent or substantial public interest set out in law (art. 9).

Remote identification adds its own rules. The applicant consents at the start to the identification, its purpose and the capture of photos, images and data, and the consent is stored with the evidence (HG 977/2023, Procedure, point 15). Data may be taken from an external source only with the applicant's consent to that source and those data categories (point 16). The record file is kept for 15 years (point 35) and the identification policy must apply data minimisation. On request, the interoperability authority tells a person which body supplied or consumed their data (Law 142/2018, art. 6(7)).

7 Sector-specific obligations

Qualified signatures for dealings with the state

Advanced electronic signatures and seals may not be used on electronic documents in legal relations between public-law entities and individuals or private legal entities (Law

124/2022, art. 22(1)(b)). In practice, anything a citizen or company signs electronically for a public authority needs a qualified signature.

State authentication and signing services

MPass is the state-owned authentication and access control service, owned by the E-Government Agency and technically administered by STISC; ministries and central authorities had to plan its integration into their services (HG 1090/2013, points 1, 3 and 4). MSign is the state integrated electronic signature service on the same model (HG 405/2014). STISC manages the Government public key infrastructure and provides public key certification and related e-signature services (Government Decision No. 414 of 8 May 2018, points 7-8 on STISC). The E-Government Agency lists the qualified signature options as the mobile signature from Orange or Moldcell (valid 2 years), the identity card and a USB token, all issued by STISC, with the EVOSign app in pilot. These services can be suspended at short notice; check egov.md.

The EVO digital identity wallet

EVO 2.0, launched on 10 June 2026, adds a digital identity wallet ("Documents" module) that the E-Government Agency describes as aligned with EU standards. Service providers integrate the wallet to receive document data and store proof of identification, and a public verifier uses a QR code that the holder approves on the phone (E-Government Agency, 10 June 2026). The identity card in the wallet is the digital version described in section 4; a full statutory wallet regime is in the bill before Parliament (section 10).

8 Risk indicators and red flags

IDENTITY ABUSE INDICATORS IN REMOTE PUBLIC-SERVICE ONBOARDING

- **Pre-recorded or replayed video**: no response to random prompts in an automated session (HG 977/2023, point 30).
- **Presentation attacks**: masks, screens or photos at the camera, the reason liveness must meet ISO/IEC 30107 level II (point 13).
- **Document or data mismatch**: a document flagged lost or stolen, or data that do not match the MRZ, chip or State Population Register (points 21, 30).
- **Degraded or non-compliant session**: low image quality, interrupted video, or refusal to follow framing instructions; each makes the identification unsuccessful (points 32, 38).
- **Misused identity copies**: identity card copies and data of living or deceased people used without consent, as the tax authority detected in purchase documents and the data protection authority confirmed.
- **Shared or orphaned credentials**: staff reusing a former employee's login to a state register, as the data protection authority found at a local public authority.
- **Leaked identity data**: the E-Government Agency reported that about one million IDNPs were queried and data sets for about 750,000 extracted (preliminary estimates) in a cyber attack on 19-23 October 2026, so name and IDNP alone prove little (egov.md, 27 October 2026).

9 Enforcement and penalties

SIS enforces Law 124/2022 mainly through status. It may suspend a qualified provider or service for a confirmed breach or false data in a conformity report, effective on publication on the SIS website (art. 37). Unremedied suspension leads to withdrawal (art. 38). SIS can also require providers to remedy breaches (art. 35(2)(m)).

A qualified provider's fault is presumed in civil claims for damage (art. 54).

Data protection fines under Law 195/2024 (art. 88) run in two tiers, whichever amount is higher: up to 1,000,000 lei or 1% of prior-year turnover for an undertaking (for example controller and processor obligations), and up to 2,000,000 lei or 2% for breaches of the core principles, including consent conditions and the special-category rules, or of a corrective order. These fines also apply to public authorities and institutions (art. 88(4)).

Only 10% of a fine applies in the first year after 23 August 2026, 40% in the second and 100% from the third (art. 90(4)).

Under the former Law 133/2011, the National Center for Personal Data Protection found that a local public authority had let staff access the real estate register's central database with a former employee's still-active credentials, kept no access log and failed to notify the Public Services Agency of user changes. It ordered revised access rights, logging and staff training (CNPDCP findings).

10 Recent changes and what to watch

- **28 October 2026**: `Bill, not enacted` Government bill No. 386 on electronic identification registered in Parliament (first reading, parlament.md). As registered, it would replace Law 124/2022 12 months after publication, have the Government designate the supervisory body and the public wallet provider, and require a certified digital identity wallet within 24 months of entry into force (art. 80).
- **28 October 2026**: `Temporary measure` after the October cyber attack, the E-Government Agency temporarily disabled MPass two-step login and EVOSign authentication; on 30 October it reported 21 public services still unavailable (egov.md).
- **11 September 2026**: `In force` SIS Order No. 67/2026 sets rules for electronic attestations of attributes issued by public bodies from authentic sources.
- **11 September 2026**: `Adopted, effective on EU accession` SIS Order No. 68/2026 on notifying e-ID schemes to the European Commission; voluntary application is allowed now.
- **23 August 2026**: `In force` Law 195/2024 replaced Law 133/2011, with fines phased in over three years.
- **23 July 2026**: `Adopted, effective on EU accession` Law 135/2026 routes cross-border data exchange through the interoperability platform (Law 142/2018, art. 11(1)).
- **10 June 2026**: `Launched` EVO 2.0 with a digital identity wallet that banks, companies and public bodies can integrate for verifier-initiated document checks.
- **April 2026**: `Proposed, consultation closed 24 Apr 2026` draft Government decision setting technical specifications for low, substantial and high assurance levels, based on EU Implementing Regulation 2015/1502.
- **18 December 2025**: `In force` the three e-ID assurance levels in art. 5^{1} of Law 124/2022, inserted by Law 117/2025, became applicable. Existing qualified providers kept their status subject to a first conformity audit.

11 What this means for identity verification

- **Documents**: design remote flows around the identity card and passport only. For a fully automated flow, NFC chip reading is mandatory, so devices without NFC need an operator-led fallback.
- **Biometrics**: match the selfie against the chip photo or the State Population Register image, not only the printed photo, and use liveness software certified to ISO/IEC 30107 at level II or above.
- **Data sources**: verify document status and data against the State Population Register; get the applicant's consent to each external source before you query it.
- **Signatures**: for anything submitted to a public authority, accept or produce a qualified signature; advanced signatures are not admitted.
- **Evidence**: keep consent, images, findings and the result in an electronic record file for 15 years, and keep a written identification policy that applies data minimisation.
- **Resilience**: support several state login options, and treat name plus IDNP as weak evidence.
- **Change**: plan for re-assessment once assurance-level criteria and the new e-ID law are adopted.

IDENTOMAT

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- Remote identity verification with ID document capture and NFC chip reading of Moldovan identity cards and passports.
- Face match against the document chip photo with biometric liveness detection to counter presentation attacks.
- Operator-led video KYC sessions for applicants whose devices cannot read the document chip.
- Consent capture, configurable workflows and an audit trail for each identification session.
- Cloud, on-premises or hybrid deployment for public-sector data residency needs.

Request a meeting

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **Legea nr. 124 din 19.05.2022 privind identificarea electronică și serviciile de încredere** [Law No. 124/2022 on electronic identification and trust services], arts. 5^1, 6, 8, 10, 21, 22, 35, 37, 38, 40, 54; last amended by Law 227/2025, in force 30 December 2025, legis.md
- **Legea nr. 117 din 29.05.2025 pentru modificarea Legii nr. 124/2022** [Law No. 117/2025 amending Law 124/2022], art. I point 4, art. II; MO 320/18.06.2025, legis.md
- **Hotărârea Guvernului nr. 977 din 06.12.2023** [Government Decision No. 977/2023 on alternative remote identification methods and the remote identification Procedure], MO 20-23/18.01.2024, legis.md

- **Hotărârea Guvernului nr. 1090 din 31.12.2013 privind serviciul MPass** [Government Decision No. 1090/2013 on MPass], last amended by HG 43/2025, legis.md
- **Hotărârea Guvernului nr. 405 din 02.06.2014 privind serviciul MSign** [Government Decision No. 405/2014 on MSign], last amended by HG 291/2024, legis.md
- **Legea nr. 273 din 09.11.1994 privind actele de identitate din sistemul național de pașapoarte** [Law No. 273/1994 on identity documents], arts. 3-4; republished MO 620-622/18.12.2025, last amended by Law 84/2026, legis.md
- **Hotărârea Guvernului nr. 125 din 18.02.2013 privind eliberarea actelor de identitate și evidența locuitorilor** [Government Decision No. 125/2013 on issuing identity documents], Annex 1, point 20^1; last amended by HG 360/2026, legis.md
- **Hotărârea Guvernului nr. 414 din 08.05.2018** [Government Decision No. 414/2018 on consolidating public-sector data centres, including STISC functions], points 7-8; last amended by HG 586/2026, legis.md
- **Legea nr. 142 din 19.07.2018 cu privire la schimbul de date și interoperabilitate** [Law No. 142/2018 on data exchange and interoperability], arts. 6, 11; art. 11(1) as amended by Law 135/2026 (in force on EU accession), legis.md
- **Legea nr. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului** [Law No. 308/2017 on AML/CFT], art. 4; last amended by Law No. 146/2026, in force 13 August 2026, legis.md
- **Legea nr. 195 din 25.07.2024 privind protecția datelor cu caracter personal** [Law No. 195/2024 on personal data protection], arts. 9, 88, 89, 90, legis.md
- **Ordinul Directorului SIS nr. 67 din 04.09.2026** [SIS Order No. 67/2026 on electronic attestations of attributes], MO 444-447/11.09.2026, legis.md
- **Ordinul Directorului SIS nr. 68 din 04.09.2026** [SIS Order No. 68/2026 on notification of e-ID schemes], MO 444-447/11.09.2026, legis.md
- **Servicii de încredere** [Trust services], Information and Security Service, sis.md
- **Semnătura electronică** [Electronic signature options], E-Government Agency, evo.gov.md
- **EVO a trecut la nivelul următor: Bine ai venit în EVO 2.0** [EVO 2.0 launch], E-Government Agency, 10 June 2026, egov.md
- **Aproximativ un milion de IDNP-uri vizate în tentative de extragere a datelor** [Cyber attack update], E-Government Agency, 27 October 2026, egov.md
- **Autentificarea în MPass prin opțiunile: doi pași și aplicația EVOSign sunt temporar dezactivate** [MPass options temporarily disabled], E-Government Agency, 28 October 2026, egov.md
- **Autoritățile verifică datele extrase neautorizat în urma atacului cibernetic** [Cyber attack update], E-Government Agency, 30 October 2026, egov.md
- **Proiect de hotărâre privind nivelurile de identificare electronică** [Draft Government decision on e-ID assurance levels], No. 324/MDED/SIS/2026, consultation 9-24 April 2026, particip.gov.md
- **Proiectul de lege privind identificarea electronică și serviciile de încredere** [Draft law on electronic identification and trust services], approved by the Government on 28 October 2026 and registered in

Parliament as No. 386, arts. 5, 80, parlament.md; earlier Government draft, April 2026, gov.md; public consultation 23 April to 8 May 2026, particip.gov.md

- **Extras din Registrul de stat al populației** [Extract from the State Population Register service], Public Services Agency, asp.gov.md
- **Constatări referitoare la încălcarea legislației** [Findings of breaches of data protection law], National Center for Personal Data Protection, datepersonale.md
- **Pagina principală** [STISC homepage], Information Technology and Cyber Security Service, stisc.gov.md