



Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Ukraine

COUNTRY **Ukraine**

INDUSTRY **Government & Public Services**

LAST UPDATED **16 October 2026**

KEY REGULATORS **Ministry of Digital Transformation of Ukraine · National Bank of Ukraine · Ukrainian Parliament Commissioner for Human Rights**

Key takeaways

- Ukraine runs public services online through Diia, the state services portal and app. A digital passport shown in Diia has the same legal force as the plastic card, and service providers may not refuse it.
- Online, a person is identified with an approved electronic identification means (for example Diia.Signature, a qualified electronic signature or bank-based BankID), each rated at a low, substantial or high assurance level. A service may only accept means that meet the level it requires.
- Fully remote first-time enrolment is limited: a qualified signature can be issued remotely only if the person already holds a substantial or high level means that was issued face to face, plus multi-factor authentication (proving identity with two different kinds of evidence).
- Anti-money laundering (AML) rules do not apply to public bodies as service providers, but private firms that supply identity means, signatures or wallets need a place on the official scheme list or trusted list and pass conformity assessment.
- Rules are moving towards the European Union (EU) digital identity wallet. A draft law and a new data protection law are still bills, not law (as of October 2026), and several measures apply only while martial law lasts.

The market is open to private providers, but on the state's terms. Public services are delivered by public bodies, while the identity layer behind them combines state infrastructure (Diia, the Unified State Demographic Register, the integrated electronic identification system) with private and bank-operated identification means that must be approved and listed.

The Ministry of Digital Transformation sets policy and keeps the lists; the Administration of the State Service of Special Communications and Information Protection supervises trust services; the National Bank of Ukraine runs BankID; and the Ukrainian Parliament Commissioner for Human Rights enforces data protection.

The biggest obstacle for a new entrant is assurance: a provider must show, through conformity assessment against the 2025 Technical Regulation, that its means meets the level it claims before any public service will accept it.

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

Ukraine is a unitary state, so identity rules for public services are national. The Cabinet of Ministers adopts most implementing acts under the Law on Electronic Identification and Electronic Trust Services.

Authority	Remit	Level	Official site
Ministry of Digital Transformation	Policy on electronic identification and trust services; keeps the list of electronic identification schemes and digital identity wallets; acts as the Central Certification Authority	National	thedigital.gov.ua
Central Certification Authority	Trusted list of qualified trust service providers; issues providers' qualified certificates	National	czo.gov.ua
Administration of the State Service of Special Communications and Information Protection	State supervision of trust services; orders and administrative fines	National	cip.gov.ua
National Bank of Ukraine (NBU)	Operates the NBU BankID System for bank-based remote identification	National	bank.gov.ua

State enterprise Diia	Operates the Diia portal and app; qualified trust service provider and electronic identification provider	National (state-owned)	diia.gov.ua
Ukrainian Parliament Commissioner for Human Rights	Data protection supervision	National	ombudsman.gov.ua
State Migration Service	Identity documents and the Unified State Demographic Register	National	dmsu.gov.ua

2 Licensing and authorisation

No licence is needed to use electronic identification as a relying party, but every private role in the identity chain needs authorisation:

Electronic identification providers

A provider may issue identification means only under a scheme included in the list of electronic identification schemes and digital identity wallets kept under Cabinet Resolution No. 218 of 27 February 2024. Cabinet Resolution No. 764 of 28 June 2024 prohibits providing means that are not on that list.

Qualified trust service providers

Providers of qualified electronic signatures are entered on the Trusted List kept by the Central Certification Authority and are supervised by the Administration of the State Service of Special Communications. Conformity assessment follows Cabinet Resolution No. 1062 of 13 September 2024.

Digital identity wallets

Wallet issuers must meet the requirements in Cabinet Resolution No. 689 of 11 June 2025 and be included in the same list as identification schemes.

BankID relying parties

A company or public body joins the NBU BankID System through an accession agreement with the National Bank. The BankID Council approves each type of service for which the system may be used, and separates commercial from non-commercial services.

Operating outside these routes has direct consequences: under the Law on Electronic Identification and Electronic Trust Services the authorities may block or cancel a provider's

qualified certificate and stop the use of an electronic identification scheme (Articles 34-9 and 34-10).

3 Identity framework (AML rules do not apply)

Law No. 361-IX of 6 December 2019 on preventing money laundering lists its reporting entities in Article 6: financial institutions, payment system operators, exchanges and designated professions and businesses. Ministries, local authorities and administrative service centres delivering public services are not among them, so there is no customer due diligence (CDD) duty for a public service as such.

What governs identity instead is a layered framework:

- **Law No. 2155-VIII on Electronic Identification and Electronic Trust Services**

In force : defines electronic identification, the three assurance levels (Article 15), digital identity wallets (Article 15-1), the list of schemes (Article 15-2), the integrated electronic identification system (Article 15-3) and recognition of foreign schemes (Article 37-1).

- **Law No. 1689-IX on the Specifics of Providing Public (Electronic Public) Services**

In force : where a law requires identifying a person who submits paper documents, electronic identification satisfies that requirement for the electronic service, and electronic documents are treated as equal to paper and plastic ones.

- **Technical Regulation on electronic identification means** (Cabinet Resolution No. 577 of 16 May 2025) **In force** : sets the proofing and authentication criteria for each assurance level.

Financial-sector due diligence still reaches public services indirectly. Under the NBU BankID Regulation, banks and non-bank payment providers acting as identifiers must identify, verify and refresh customer data under financial monitoring law, at least every five years, before passing it to a government relying party.

4 Identity verification and onboarding

Assurance levels

Article 15 of Law No. 2155-VIII requires each scheme to provide a low, substantial or high level of assurance. The 2025 Technical Regulation sets the criteria: a low level rests on information that allows the person to be identified; a substantial level requires at least two authentication factors; and a high level adds confirmation that the person is the one to

whom photographs or biometric data held by the state belong (digitised fingerprints excluded). The authoritative sources are identity documents and identification data in the Ministry of Internal Affairs' unified information system.

Approved schemes

Cabinet Resolution No. 1276 of 5 December 2023 lists the state enterprise Diia's schemes: Diia.Signature (scheme DIIA.PKI.Remote) and a qualified signature on any medium (DIIA.PKI) at high assurance, plus identification through NBU BankID (DIIA.Oauth). The integrated electronic identification system (Cabinet Resolution No. 1150 of 3 November 2023) is the hub through which public portals accept these means.

Documents and registers

For face-to-face enrolment the Diia trust service provider checks the person against the Unified State Demographic Register and a citizen's passport, passport for travel abroad, or permanent or temporary residence permit; foreigners without these may use a legalised national passport. Data are cross-checked with the demographic, taxpayer, civil status and business registers through the integrated system. Law No. 5492-VI defines biometric data (digitised signature, facial image and fingerprints) and requires the contactless chip in identity documents to carry them.

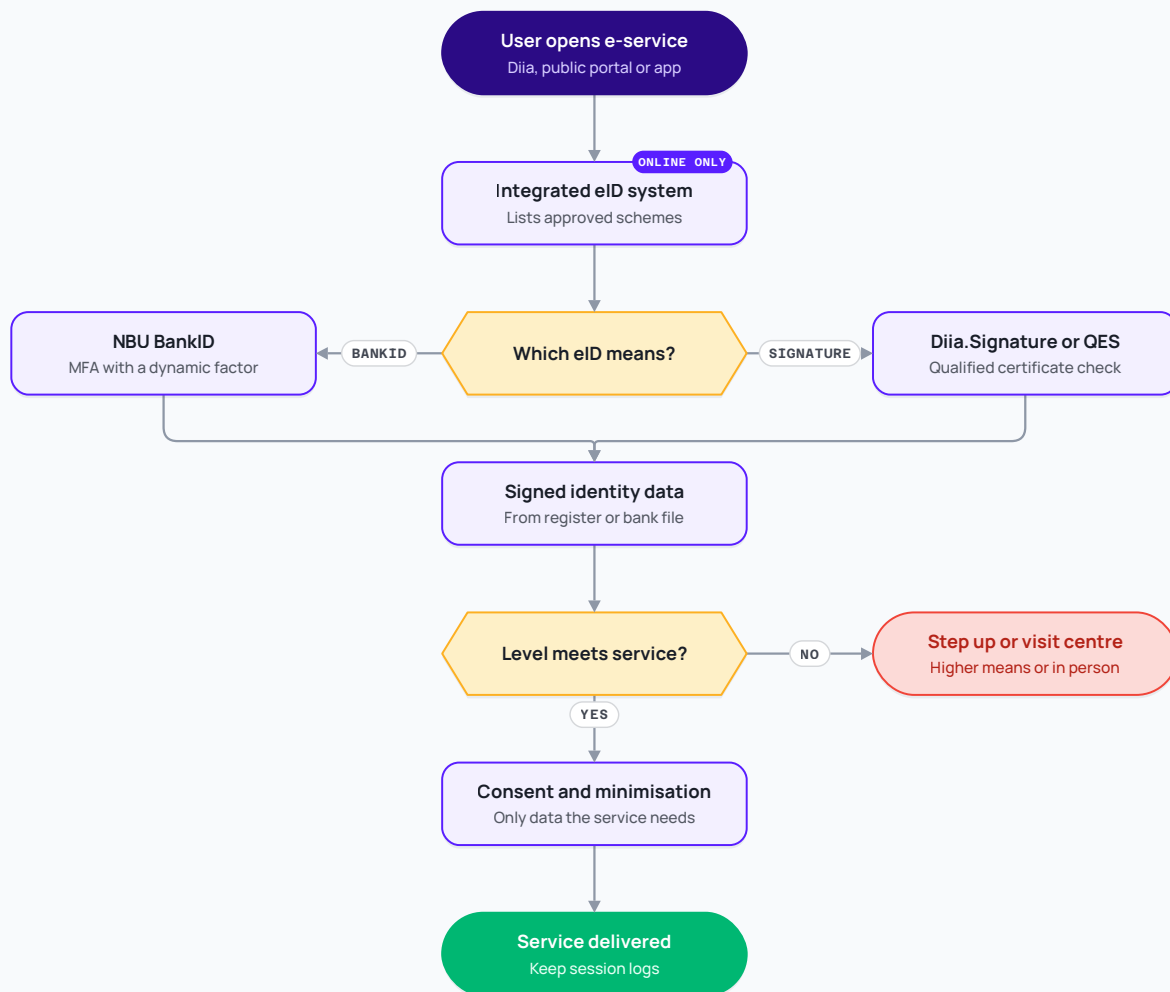


Figure 1. Remote electronic identification for a public e-service in Ukraine.

5

Digital channels: what's different

Bottom line: online identity carries the same legal weight as a paper or plastic document, but a remote credential at substantial or high assurance must normally trace back to a face-to-face check or to a bank's own customer due diligence.

Requirement	In person / centre	Online / remote	Difference
Legal force of the ID document	Plastic or paper passport	Digital passport in Diia	Same

How identity is established	Document check by an official	Approved electronic identification means	Differs
Assurance level	Not graded	Low, substantial or high per scheme	Differs
Getting a qualified signature	Register and document check	Only with an earlier in-person means plus MFA	Differs
Bank-based identity	Not used	BankID, MFA with a dynamic factor	Differs
Record keeping by the signature provider	Permanent storage	Permanent storage	Same
Data protection regime	Law No. 2297-VI	Law No. 2297-VI	Same

Remote issuance rests on an earlier in-person check

The Diia trust service provider identifies an applicant for a qualified certificate in one of four ways: in person against the demographic register and an identity document; remotely, using a high or substantial level means previously issued face to face, together with multi-factor authentication; through a still-valid qualified certificate issued by either route; or by another method set by law whose reliability a conformity assessment body confirms as equivalent to physical presence.

BankID brings in the bank's due diligence

The NBU BankID Regulation, restated by NBU Board Resolution No. 1 of 8 January 2026, requires multi-factor authentication with at least one dynamic factor for every request. A bank may change the phone number used for authentication remotely only if it suspends BankID for that user for 24 hours and notifies both numbers.

Digital documents are equal

Law No. 1368-IX of 30 March 2021 gave the digital ID card and biometric passport in Diia the same legal force as the physical documents, and Law No. 1689-IX bars public service providers and businesses from refusing a service because the person does not carry paper documents.

Pending

A Ministry draft law implementing the European Digital Identity Framework was scheduled for public consultation on 30 July 2026 **Draft, consultation**.

6

Data protection and biometrics

The Law on Personal Data Protection, No. 2297-VI of 1 June 2010, applies to all identity capture, and the Ukrainian Parliament Commissioner for Human Rights supervises it. For public e-services three points matter. First, under the BankID Regulation a relying party must tell the user which data it will request and why, obtain consent before the request, use only the standardised data set approved for its service type, and may not sell or pass on the data. Second, identity providers must notify users of security breaches affecting them within two hours and the supervisor within 24 hours, a rule found both in the Diia certificate policy and in the BankID Regulation. Third, facial images and other biometric data are held by the state in the demographic register and on document chips under Law No. 5492-VI; high-level assurance uses them for matching rather than requiring private providers to build their own biometric databases.

Bill No. 8153, a new data protection law aligned with the EU General Data Protection Regulation, passed first reading on 20 November 2024 **Bill, first reading only**.

7

Sector-specific obligations

No paper where the state already holds the data

Law No. 1689-IX requires public bodies to obtain documents and information held in state information systems themselves, free of charge, rather than asking the applicant. Onboarding flows for public services should therefore request only what no register can supply.

Trust services inside public bodies

Cabinet Resolution No. 798 of 1 August 2023 sets the procedure for using electronic trust services in state authorities, local governments and state-owned enterprises, and Resolution No. 1298 of 12 December 2023 sets the advanced signature formats accepted for electronic public services.

Wallets and the Diia pilot

Cabinet Resolution No. 1400 of 24 October 2025 runs an experimental project in which the Diia app works as a digital identity wallet issuing electronic attestations of identity data and attributes. The attestation can be presented wherever legislation requires a passport, and the pilot provides for recognising European digital identity wallets issued under EU Regulation No. 910/2014.

Martial-law measures

Cabinet Resolution No. 248 of 10 March 2022 allows the eDocument in Diia, which includes the person's facial image, to be presented for the period of martial law only. Ukrainian passport cards that expired during martial law also remain valid identity documents for that period.

8

Risk indicators and red flags

IDENTITY-ABUSE INDICATORS DRAWN FROM UKRAINIAN RULES

- **Recent phone number change:** a new authentication number shortly before an identification request (BankID suspends use for 24 hours).
- **Compromised credentials:** suspected unlawful use of BankID access data, which must be blocked immediately.
- **Stale identity data:** identity document invalidated or customer data not refreshed, which suspends BankID.
- **Over-collection:** a relying party requesting more than the approved data set for its service.
- **Data on-sale:** identity data obtained through BankID being sold or passed to third parties.
- **Key compromise:** a signature private key or password disclosed or used after blocking.
- **Certificate data mismatch:** wrong identity data in a newly issued qualified certificate, to be reported within 24 hours.
- **Expired document:** a document presented as valid outside a martial-law exemption.

Enforcement runs on three tracks:

- **Trust services and electronic identification.** The Administration of the State Service of Special Communications carries out state control, issues orders to remedy breaches and imposes administrative fines; Law No. 2155-VIII also provides for off-site supervision (Article 34-1), blocking or cancelling a qualified provider's certificate (Article 34-9) and stopping the use of a scheme (Article 34-10).
- **BankID.** The National Bank may suspend a participant or its node until a breach is fixed, and the BankID Council applies contractual fines; participants are liable in full for damage caused to users.
- **Data protection.** The Commissioner draws up administrative offence reports under Article 188-39 of the Code of Administrative Offences and sends them to court. Fines are set in multiples of the non-taxable minimum income of citizens and differ for citizens and officials. In June 2023 the Commissioner filed a report against an official of the Novomoskovsk city council's executive committee for publishing an applicant's personal data online without anonymisation.

- **1 September 2026** Bill, first reading only : Verkhovna Rada Resolution No. 4958-IX put Bill No. 8153 (data protection) and Bill No. 12174 (amendments to Law No. 2155-VIII) on the session agenda; both await second reading, so plan for the current rules.
- **July 2026** Draft, consultation : the Ministry of Digital Transformation scheduled consultations on a draft law implementing the European Digital Identity Framework and on a pilot for mutual recognition of trust services with the EU; wallet-based flows are likely to expand.
- **30 June 2026** In force : deadline for BankID identifier banks to comply with the restated BankID Regulation, with reports due to the NBU by 1 August 2026; expect stricter authentication and data refresh.
- **24 October 2025** In force, pilot : Cabinet Resolution No. 1400 launched the Diia digital identity wallet pilot with recognition of European wallets.
- **11 June 2025** In force : Cabinet Resolution No. 689 set requirements for issuing digital identity wallets.
- **16 May 2025** In force : Cabinet Resolution No. 577 approved the Technical Regulation on assurance levels, the benchmark for every conformity assessment.

What this means for identity verification

Design for federation first: a public e-service in Ukraine normally accepts identity from approved schemes through the integrated system rather than running its own document and selfie check. A private provider that wants its own means accepted must be listed and must prove the claimed assurance level under the 2025 Technical Regulation.

Map each service to an assurance level and offer a step-up path, for example from BankID to a qualified signature, or to an administrative service centre. Accept digital documents from Diia and verify them through Diia's own checks rather than images. Build for foreigners separately, since they may lack Ukrainian documents and register entries. Keep identification logs (BankID participants must hold request data for at least five years) and expect re-verification when a bank refreshes customer data or a phone number changes. Track the end of martial law, which will remove the eDocument and the expired-passport exemption.

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:

- ID document capture and verification, including NFC chip reading, for services that must check Ukrainian ID cards, biometric passports and residence permits.
- Biometric liveness and face match to support step-up checks where a service requires a higher assurance level.
- No-code workflow builder to route users between eID methods, step-up paths and in-person fallbacks.
- E-signatures and an audit trail for each identification event, supporting log retention duties.
- 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

- Закон України «Про електронну ідентифікацію та електронні довірчі послуги» [Law on Electronic Identification and Electronic Trust Services], No. 2155-VIII of 5 October 2017, edition of 18 December 2024, Articles 15, 15-1, 15-2, 15-3, 34-1, 34-9, 34-10, 37-1, zakon.rada.gov.ua
- Закон України «Про особливості надання публічних (електронних публічних) послуг» [Law on the Specifics of Providing Public (Electronic Public) Services], No. 1689-IX of 15 July 2021, edition of 2 September 2024, zakon.rada.gov.ua
- Закон України «Про Єдиний державний демографічний реєстр...» [Law on the Unified State Demographic Register and Identity Documents], No. 5492-VI of 20 November 2012, zakon.rada.gov.ua
- Law No. 1368-IX of 30 March 2021 (digital passports) and Law No. 1689-IX, as listed by Diia Paperless, Legislation page, paperless.diia.gov.ua
- Закон України «Про запобігання та протидію легалізації (відмиванню) доходів...» [Law on Prevention of Money Laundering], No. 361-IX of 6 December 2019, Article 6, zakon.rada.gov.ua
- Закон України «Про захист персональних даних» [Law on Personal Data Protection], No. 2297-VI of 1 June 2010, zakon.rada.gov.ua
- Cabinet of Ministers Resolution No. 577 of 16 May 2025, Technical Regulation on requirements for electronic identification means and assurance levels, zakon.rada.gov.ua
- Cabinet of Ministers Resolution No. 689 of 11 June 2025, requirements for issuing digital identity wallets, zakon.rada.gov.ua
- Cabinet of Ministers Resolution No. 1400 of 24 October 2025, experimental project on the Diia digital identity wallet, zakon.rada.gov.ua
- Cabinet of Ministers Resolution No. 218 of 27 February 2024, procedure for the list of electronic identification schemes and digital identity wallets, zakon.rada.gov.ua
- Cabinet of Ministers Resolution No. 248 of 10 March 2022, use of the eDocument during martial law, zakon.rada.gov.ua
- Central Certification Authority, Normative legal acts (list of Cabinet resolutions Nos. 798/2023, 1150/2023, 1298/2023, 764/2024, 1062/2024 and others), czo.gov.ua
- Cabinet of Ministers, news of 5 December 2023 on Resolution No. 1276 approving electronic identification schemes, kmu.gov.ua

- Регламент роботи КНЕДП «Дія» [Operating Regulation and Certificate Policy of the Qualified Trust Service Provider Diia], sections 1.4, 3.2.2, 4.4, ca.diia.gov.ua
- NBU Board Resolution No. 1 of 8 January 2026 restating the Regulation on the NBU BankID System (Resolution No. 32 of 17 March 2020), officially published 9 January 2026, bank.gov.ua
- Verkhovna Rada bill card No. 8153, draft Law on Personal Data Protection, itd.rada.gov.ua
- Verkhovna Rada bill card No. 12174, amendments to the Law on Electronic Identification and Electronic Trust Services, itd.rada.gov.ua
- Ministry of Digital Transformation, planned public consultations for July 2026, thedigital.gov.ua
- Ukrainian Parliament Commissioner for Human Rights, news of 7 June 2023 on an administrative offence report (Novomoskovsk city council), ombudsman.gov.ua
- Cabinet of Ministers, news on the validity of passports that expired during martial law, kmu.gov.ua