



Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Poland

COUNTRY **Poland**

INDUSTRY **Government & Public Services**

LAST UPDATED **20 October 2026**

KEY REGULATORS **Minister of Digital Affairs · Minister of the Interior and Administration · President of the Personal Data Protection Office**

Key takeaways

- Poland's state digital identity is open to private companies, but only through the government's own gates: you need the Minister of Digital Affairs' consent to accept state logins (login.gov.pl) or to offer a service inside the mObywatel app.
 - Private online services may log users in with the e-ID card (the chip identity card) or the mObywatel profile. The Trusted Profile (Profil Zaufany), the most widely held state login, is for public bodies only.
 - The mDowód (the identity document in the mObywatel app) replaces the plastic identity card only face to face. It cannot be used to identify someone remotely, and it cannot be used at the border.
 - Since 30 June 2026, banks, payment firms, telecom operators, lenders and other listed firms can check identity card data against the state register and receive the card's official photo for a face match, free of charge.
 - An EU Digital Identity Wallet is due inside mObywatel as a pilot in December 2026, and many regulated firms must accept such wallets on request from late 2027.
-

The market is open: no licence is needed to build identity services on top of Polish public digital identity, but every connection to state systems is a consent or decision of the Minister of Digital Affairs, with security, testing and data protection conditions attached. Public bodies themselves are not covered by the anti-money laundering regime; identity in this sector is governed by the identity card, mObywatel, informatisation and trust services statutes.

The principal authorities are the Minister of Digital Affairs, who runs mObywatel, the Trusted Profile, the national electronic identification node and the PESEL reservation register and supervises trust services, and the Minister of the Interior and Administration, who personalises identity cards. The biggest obstacle for a new entrant is that the strongest state credentials are channel-specific: what works at a counter (mDowód) does not work online, and what works online for public services (Trusted Profile) is closed to private relying parties.

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
Minister of Digital Affairs (Minister Cyfryzacji)	mObywatel app and mDowód, Trusted Profile, national electronic identification node, PESEL reservation register, supervision of trust service providers and of the national eID scheme	National	gov.pl/web/cyfryzacja
Minister of the Interior and Administration (MSWiA)	Identity card law, personalisation of identity cards, supervision of voivodes in identity card matters	National	gov.pl/web/mswia
Municipal authorities (wójt, burmistrz, prezydent miasta)	Issuing identity cards; registering PESEL reservations in person	Local (delegated state task)	Each municipality
President of the Personal Data Protection Office (UODO)	Data protection supervision, including biometric processing	National	uodo.gov.pl
European Union (eIDAS Regulation)	Electronic identification, trust services and the EU Digital Identity Wallet	Supranational	eur-lex.europa.eu

The Head of the Internal Security Agency (ABW) also gives opinions on identity scheme operators that apply to join the national node, under the Act on Trust Services and Electronic Identification.

2 Licensing and authorisation

No licence is required to verify identity in Poland. What requires permission is access to state identity infrastructure, and each gate has its own procedure.

Joining the national node as a relying party

A business that wants to accept state electronic identification means applies to the Minister of Digital Affairs. Consent follows an information security management system meeting Article 8 of the National Cybersecurity System Act, positive integration tests, a data protection statement and, for non-public entities, a demonstrated factual interest assessed against security and the public interest (Act on Trust Services and Electronic Identification, Art. 21t and 21u). The applicant states the assurance level each online service needs.

Joining the node as an identity provider

A bank or other firm issuing its own eID means needs a connection decision: its means must meet the eIDAS assurance-level requirements, pass integration tests, run an information security management system, carry civil liability insurance and, where triggered, receive a positive ABW opinion (Art. 21b and 21g). Liability toward public services is capped at EUR 2,000,000 per year for all events, except in cross-border authentication (Art. 21ca).

Offering a service in mObywatel

Public and private entities may provide services in the app with the Minister's consent, after accepting the general terms for that service, including security conditions added in 2025 (Act on the mObywatel Application, Art. 15). Refusal and withdrawal of consent are administrative decisions, and withdrawal is immediately enforceable (Art. 15(8) to (11)).

Access to state registers

Verification of identity card data in the Register of Identity Cards is available to any entity with a factual interest that logs access and secures the data, for a fee where it performs no public task (Identity Cards Act, Art. 68). Photo access and PESEL reservation checks are limited to entities listed in the statutes (Art. 68a; Population Register Act, Art. 23m).

Operating outside these permissions is not a licensing offence, but it removes access: the Minister suspends node authentication for a system that breaches the node security

policy and disconnects it if the cause is not removed within three months (Act on Trust Services and Electronic Identification, Art. 39g and 39h).

3 Identity framework (AML rules do not apply)

The Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing lists its obliged institutions in Article 2(1): banks, payment and e-money institutions, investment firms, insurers, virtual currency providers, notaries and other financial and professional businesses. Public authorities delivering public services, and the state's digital identity schemes as such, are not on that list. A bank that issues eID means remains an obliged institution in its banking capacity, but the identity scheme rules below apply to it as a scheme operator.

Identity in this sector rests on four statutes:

- **Identity Cards Act (2010)**. The identity card confirms identity and Polish citizenship in Poland and in EU, EEA and free-movement states, and every adult citizen living in Poland must hold one (Art. 4 and 5). Cards are valid for 10 years from age 12, and 5 years below that (Art. 7).
- **Act on the mObywatel Application (2023)**. Where the law requires identity or citizenship to be established from an identity document, the mObywatel document satisfies that requirement (Art. 7(4)).
- **Act on the Informatisation of Entities Performing Public Tasks (2005)**. Public online services must authenticate users with an eID means from a scheme connected to the national node, a notified EU scheme, or a qualified certificate (Art. 20a).
- **Act on Trust Services and Electronic Identification (2016)**. It creates the national eID scheme and node, and implements eIDAS.

There is no customer due diligence regime, no beneficial ownership duty and no suspicious transaction reporting for public services. Sanctions screening is not an obligation of public service onboarding.

4 Identity verification and onboarding

The state credentials

Credential	What it proves	Who may rely on it
------------	----------------	--------------------

Identity card (e-dowód)	Graphic layer plus a chip holding personal data, facial image, fingerprints (from age 12) and certificates for authentication, the personal signature and presence confirmation; it is a qualified signature creation device	Anyone in person; online via the personal profile, including private entities
mObywatel document (mDowód)	Identity and Polish citizenship, issued for 5 years with name, PESEL, date of birth, citizenship, parents' names and the identity card photo	Anyone, in physical presence only
mObywatel profile	Name, date of birth and PESEL, with at least two authentication factors from different categories	Public and private online services
Trusted Profile	Name, date of birth and PESEL, checked automatically against the PESEL register	Public online services

Documentary and register checks

An mObywatel document presented for verification carries the holder's electronic signature, and the verifier may check its data, the Minister's advanced electronic seal, the holder's signature, its visual security features or the working of the service (mObywatel Act, Art. 9). For the plastic card, the graphic layer can be confirmed against the chip (Identity Cards Act, Art. 10a(2)).

Remote document checks rely on the Register of Identity Cards. An authorised entity submits name, PESEL, card series and number, issue date and expiry date and receives a match result; since 30 June 2026 a failed match returns a report naming which field failed and whether the card has been invalidated (Art. 68). After a positive match, listed firms receive the photo from the holder's latest valid card for comparison with the applicant (Art. 68a).

Biometrics and fingerprints

Fingerprints in the identity card chip may be read only by the public bodies listed in Article 66(3) of the Identity Cards Act (Art. 12ca). Private firms can use facial comparison against the register photo, but not fingerprint verification.

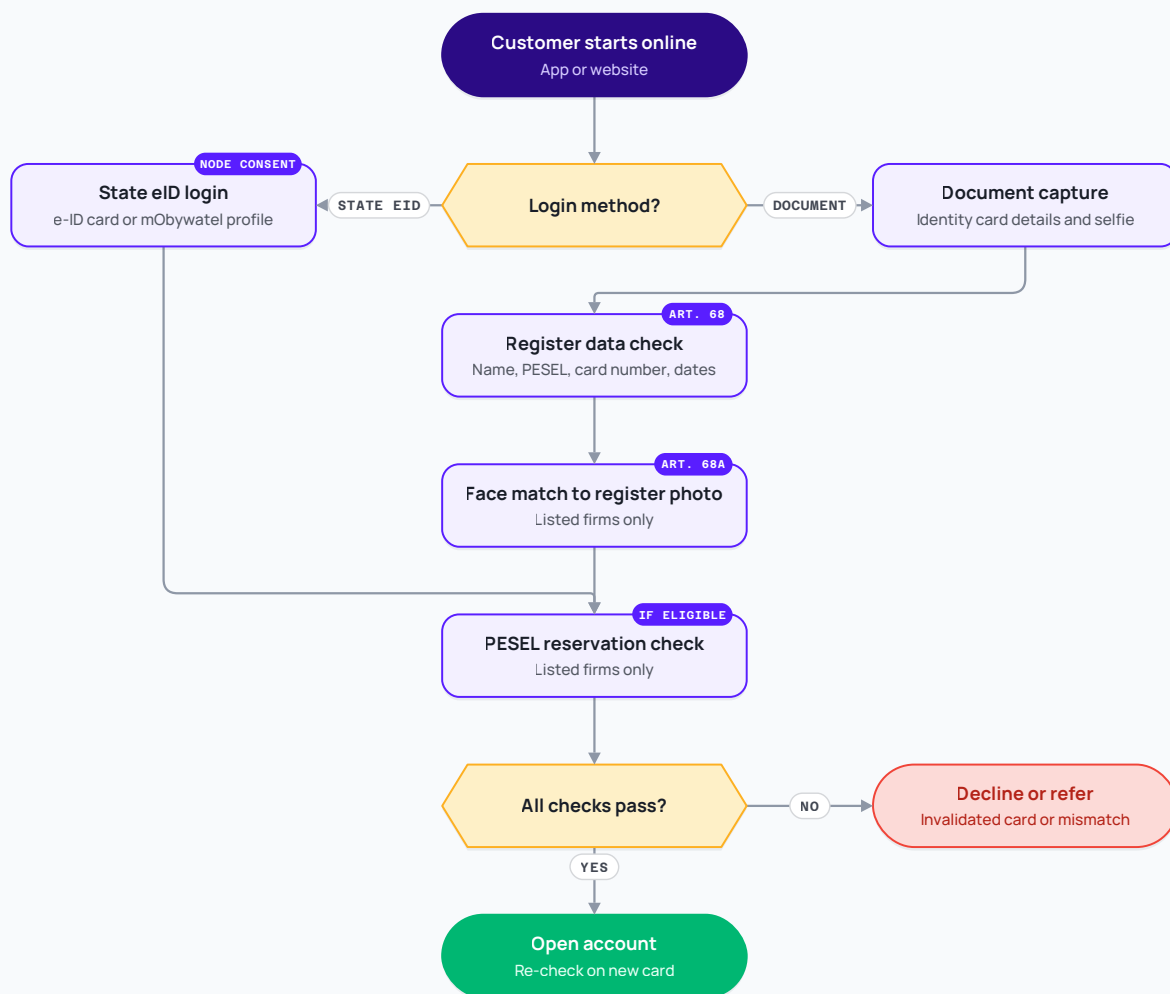


Figure 1. Remote onboarding of a Polish citizen by a private service using state identity infrastructure.

Relying parties connected to the node choose the assurance level each service requires (Act on Trust Services and Electronic Identification, Art. 21a(4) and 25); Polish law does not fix one level for private services.

5 Digital channels: what's different

Bottom line: Polish state identity is deliberately split by channel: the mDowód replaces the identity card only face to face, and online identification runs through eID means on the national node, of which the Trusted Profile is reserved for public bodies.

Requirement	In person	Online / remote	Difference
Accepted state credential	Identity card, passport or mDowód	eID means (personal profile, mObywatel profile, Trusted Profile) or a qualified certificate	Differs
Use of mDowód	Equivalent to the identity card	Not an online identification means	Differs
Who may rely on the credential	Anyone shown the document	Trusted Profile: public bodies only; personal and mObywatel profiles: private entities too	Differs
Permission to use state systems	None to inspect a document	Minister's consent to join the node or offer an mObywatel service	Differs
Assurance level	Not applicable	Set by the relying party per service	Differs
Register check of card data	Available (Art. 68)	Available (Art. 68)	Same
PESEL reservation check	Available to listed entities	Available to listed entities	Same
Trusted Profile confirmation	At a confirmation point with identity card or passport	Bank eID, qualified signature, personal profile or video identification	Differs
Signing	Handwritten signature	Trusted signature or personal signature; the personal signature binds private parties only by agreement	Differs

The mDowód is an in-person document

The Act defines the mObywatel document as proving identity and citizenship in Poland "in relations of mutual physical presence of the parties" (Art. 2(8)). It does not entitle the holder to cross the border, and it may not be used where circumstances prevent the necessary level of certainty (Art. 7(5)). Online services need a different credential.

Private access to state eID

The Minister's eID system lets public bodies authenticate with the Trusted Profile, the personal profile and the mObywatel profile, while entities other than public bodies may use only the personal profile and the mObywatel profile (Informatisation Act, Art. 20aa(1)). Authentication through the node is free for public bodies (Act on Trust Services and Electronic Identification, Art. 21a(3)).

Remote Trusted Profile confirmation by video

The Minister may confirm a Trusted Profile by video identification: the applicant's live image is compared with the photo in the Register of Identity Cards, the identity card or passport is shown on camera, and knowledge questions from public registers may be added. The session is recorded and the recording is kept for 6 years (Informatisation Act, Art. 20cb).

Pending: the EU Digital Identity Wallet

Regulation (EU) 2024/1183 **Adopted, wallets due by end 2026** requires each Member State to provide a wallet. The Ministry of Digital Affairs plans a pilot inside mObywatel in December 2026, activated once with an e-ID card; without a chip identity card the wallet cannot be used (Ministry of Digital Affairs, 4 March 2026).

6 Data protection and biometrics

The GDPR applies directly to identity capture, and the Polish identity statutes cite it expressly; the Act of 10 May 2018 on the Protection of Personal Data supplements it, under the supervision of UODO. What is specific to this sector is that the statutes fix the controllers, data sets and retention periods themselves.

- **mObywatel.** The Minister of Digital Affairs is the controller of users' data in the mObywatel system and keeps it for 6 years after the user certificate expires or is revoked, and for 20 years after the mObywatel profile is revoked for data in the eID system (Art. 20).
- **Register photo.** The photo is released only after a positive data match and only from the latest valid card (Identity Cards Act, Art. 68a(1) and (4)). Firms receiving it handle biometric data for identity verification and need a lawful basis under the GDPR for the comparison.
- **Fingerprints.** Reserved to listed public bodies (Art. 12ca).

- **Video identification.** Recordings are kept for 6 years (Informatisation Act, Art. 20cb(5)).
- **PESEL reservation checks.** System logs are kept for 6 years, and every person can see who checked their number and when (Population Register Act, Art. 23c(4) and 23l).
- **eID usage data.** Unauthorised collection, processing or copying of data on the use of an eID means connected to the node carries a fine of up to PLN 1,000,000 (Act on Trust Services and Electronic Identification, Art. 47a).

7 Sector-specific obligations

The PESEL reservation register

Any adult can block (reserve) their PESEL number free of charge online, at any municipality, or where offered at a bank, credit union or the designated postal operator, and can lift it temporarily (Population Register Act, Art. 23d to 23f). Reservation is automatic when an identity card is reported lost or a suspected misuse of personal data is reported (Art. 23g). Anyone can check a reservation after authenticating and entering the PESEL plus the latest identity document number, declaring under criminal liability on whose behalf they act (Art. 23j). Banks, credit unions, notaries, telecom providers, consumer lenders, listed payment providers, credit bureaus and insurers receive the data by automated verification (Art. 23m).

Electronic signatures tied to state identity

A trusted signature has the legal effect of a handwritten signature unless other provisions say otherwise (Informatisation Act, Art. 20ae). A personal signature made with the identity card has that effect toward public bodies, and toward other parties only if both agree (Identity Cards Act, Art. 12d).

Duties of eID holders and operators

Holders of eID means on the national node must report loss, theft or loss of exclusive control without delay, and are not liable for obligations incurred after reporting (Act on Trust Services and Electronic Identification, Art. 21e and 21f). Operators of notified schemes report security breaches to the Minister within 24 hours (Art. 26(2)). Since 3 April 2026, trust service providers entered in the register are also recorded as key or important entities under the National Cybersecurity System Act (Dz.U. 2026 poz. 252, Art. 15).

Risk indicators and red flags

IDENTITY ABUSE INDICATORS DRAWN FROM POLISH IDENTITY LAW

- **Reserved PESEL:** the applicant's number is reserved at the time of the transaction.
- **Invalidated card:** the register reports the identity card as invalidated, often after loss or a misuse report.
- **Partial data mismatch:** name and PESEL match but card series, issue date or expiry do not.
- **Face differs from register photo:** the live image does not match the latest card photo.
- **Someone else's eID:** logins using another person's eID means, a criminal offence under Art. 40a of the trust services act.
- **Lost control of credentials:** signals that an eID means is not under the holder's exclusive control.
- **mDowód offered remotely:** an mObywatel document shown as a screenshot or over video, outside physical presence.

Enforcement and penalties

Penalties in this sector are set by the Act on Trust Services and Electronic Identification and imposed by decision of the Minister of Digital Affairs, who weighs the scope, duration and effects of the breach (Art. 47 and 48).

Breach	Penalty	Provision
Qualified trust service provider breaches (policy, certificates, reporting, audits)	Up to PLN 50,000 per breach type; up to PLN 10,000 for no termination plan; up to PLN 100,000 for failing termination duties	Art. 46 and 47(2)
Unauthorised collection or processing of eID usage data	Up to PLN 1,000,000	Art. 47a

Scheme operator knowingly allowing authentication with a means not under the holder's control	Up to PLN 1,000,000	Art. 47b
Using someone else's eID means, or signing with another person's signature data	Fine, restriction of liberty or up to 3 years' imprisonment	Art. 40 and 40a
Node security breach by a connected system	Suspension; disconnection if not cured within 3 months	Art. 39c to 39h

Withdrawal of consent to provide an mObywatel service is immediately enforceable (mObywatel Act, Art. 15(11) and 16(13)). Breaches of the GDPR in identity processing are enforced separately by UODO.

10 Recent changes and what to watch

- **11 January 2027** Adopted, effective 11 Jan 2027 Branches of non-EU banks join the entities entitled to PESEL reservation checks and register photos (Dz.U. 2026 poz. 1206, Art. 19 and 20).
- **December 2026** Adopted, wallets due by end 2026 EU Digital Identity Wallet pilot planned in mObywatel; firms should prepare to accept wallet credentials as well as existing eID means.
- **8 October 2026** Bill, not enacted The Sejm passed a bill giving insurers access to identity card series, number and expiry from the PESEL register after a card is replaced; it awaits the Senate and the President.
- **30 June 2026** In force Register photo access and mismatch reports for listed firms (Identity Cards Act, Art. 68(1b) and 68a), added by Dz.U. 2025 poz. 1006.
- **3 April 2026** In force Node connection now requires a security management system under the National Cybersecurity System Act (Dz.U. 2026 poz. 252).
- **12 August 2025** In force mObywatel services gained security conditions and powers to suspend and withdraw consent (Dz.U. 2025 poz. 1019).

Under Article 5f of the amended eIDAS Regulation, private relying parties that must use strong user authentication, other than micro and small enterprises, must also accept EU wallets on the user's request no later than 36 months after the wallet implementing acts entered into force.

- **Design two paths.** A state eID login path (e-ID card personal profile or mObywatel profile through the node) and a document path for users without them. Do not plan on the Trusted Profile for a private service.
- **Never accept the mDowód remotely.** It is valid only in physical presence; for in-person flows, verify its seal or signature rather than its appearance alone.
- **Use the registers where you are eligible.** Card data checks (Art. 68) are open to any entity with a factual interest; photo comparison (Art. 68a) and PESEL reservation checks (Art. 23m) only to listed sectors.
- **NFC reading.** The identity card chip carries signed personal data and a facial image, but fingerprints stay reserved to public bodies.
- **Retention.** Align logs and recordings with the statutory 6-year periods where you act in a state process, and minimise elsewhere.
- **Re-verification triggers.** A new identity card, a reported loss, a PESEL reservation or an expired mObywatel certificate.
- **Foreign residents.** The mDowód, Trusted Profile video route and personal profile serve Polish citizens; foreigners need passport or residence document checks.

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 reading of the Polish identity card chip, for users who do not log in with a state eID.
- Biometric liveness and face match, to compare the applicant with the identity card photo before any register-based comparison.
- No-code workflow builder to run a state eID path and a document path side by side, with re-verification when a new card is issued.
- Audit trail and configurable retention for each check, aligned with the evidence a firm must keep.

[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

- Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel [Act on the mObywatel Application], consolidated text Dz.U. 2026 poz. 1232, Art. 2, 7, 9, 14, 15, 16, 20, dziennikustaw.gov.pl
- Ustawa z dnia 9 lipca 2025 r. o zmianie ustawy o aplikacji mObywatel oraz niektórych innych ustaw [amending act], Dz.U. 2025 poz. 1019, dziennikustaw.gov.pl
- Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych [Identity Cards Act], consolidated text Dz.U. 2025 poz. 1753, Art. 4, 5, 7, 10a, 12a, 12ca, 12d, 48a, 68, 68a, dziennikustaw.gov.pl
- Ustawa z dnia 25 czerwca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw [amending act], Dz.U. 2025 poz. 1006, dziennikustaw.gov.pl

- **Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne** [Informatisation Act], consolidated text Dz.U. 2026 poz. 1241, Art. 20a to 20e, dziennikustaw.gov.pl
- **Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej** [Act on Trust Services and Electronic Identification], consolidated text Dz.U. 2024 poz. 1725, Art. 21a to 26, 39a to 49, dziennikustaw.gov.pl
- **Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw** [cybersecurity amending act], Dz.U. 2026 poz. 252, Art. 15, dziennikustaw.gov.pl
- **Ustawa z dnia 24 września 2010 r. o ewidencji ludności** [Population Register Act], consolidated text Dz.U. 2026 poz. 384, Art. 23a to 23p, dziennikustaw.gov.pl
- **Ustawa z dnia 31 lipca 2026 r. o zmianie ustawy – Prawo bankowe oraz niektórych innych ustaw** [Banking Law amending act], Dz.U. 2026 poz. 1206, Art. 19, 20, 57, dziennikustaw.gov.pl
- **Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu** [AML Act], consolidated text Dz.U. 2025 poz. 644, Art. 2(1), dziennikustaw.gov.pl
- **Rządowy projekt ustawy o zmianie ustawy o ewidencji ludności** [government bill amending the Population Register Act], Sejm print 2996, sejm.gov.pl
- **Regulation (EU) 2024/1183** amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, OJ L 30.4.2024, Art. 5a and 5f, eur-lex.europa.eu
- **Europejski portfel tożsamości cyfrowej zmierza do mObywatela** [EU digital identity wallet heading to mObywatel], Ministry of Digital Affairs, 4 March 2026, gov.pl