Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Germany

COUNTRY Germany

INDUSTRY Government & Public Services

LAST UPDATED 30 October 2026

KEY REGULATORS Federal Ministry for Digital Affairs and State Modernisation · Federal Ministry of the Interior · Federal Office for Information Security

Key takeaways

- German public services identify people online mainly through the chip in the national ID card (the "Online-Ausweis"), unlocked with a six-digit PIN. For services that need the highest level of assurance, this or an equivalent EU-recognised electronic ID is required.
- Any company that wants to read identity data from the ID card chip, online or at a counter, needs a state authorisation from the Federal Office of Administration. Requesting chip data without one can cost a fine of up to EUR 30,000.
- Online, the central citizen account (BundID) replaces handwritten signatures for many forms once the user has proved their identity. In person, the ID card itself must still be applied for at the local ID office.
- Germany's state digital identity wallet, "d-you", is due to launch on 2 January 2027. The law that would let it count wherever the ID card's online function is accepted passed the Bundestag (the federal parliament) in October 2026 but is not yet law.
- Businesses that want to accept EU digital identity wallets must register as relying parties under EU rules that apply from 24 December 2026. From December 2027, larger firms that must use strong authentication must also accept the wallets if a user asks.

Germany is open to private identity providers, but on its own terms: the state issues the identity, and private firms plug into it under an authorisation regime rather than replacing it. Public authorities are not obliged entities under the anti-money laundering law, so identity in this sector is governed by identity card law, the Online Access Act and the EU eIDAS Regulation instead.

The principal authorities are the Federal Ministry for Digital Affairs and State Modernisation (digital identity, the citizen account and the wallet), the Federal Ministry of the Interior (identity documents) and the Federal Office for Information Security (technical standards and assurance levels).

The biggest obstacle for a new entrant is the fixed list of accepted methods: for public services at the "high" level, only state eIDs and notified EU schemes count, and video identification or document-and-selfie checks are not among them.

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

Identity law is federal; the 16 Länder (states) run local ID offices and portals.

Authority	Remit	Level	Official source
Federal Ministry for Digital Affairs and State Modernisation (BMDS)	Digital administration and steering of the Online Access Act, BundID citizen account, EU digital identity wallet "d-you"	Federal	bmds.bund.de
Federal Ministry of the Interior (BMI)	Passports, ID cards and identity management, which stayed with the BMI when BMDS was created in 2025; designates the authorisation certificate office	Federal	Organisational decree, 2025

Vergabestelle für Berechtigungszertifikate (VfB) at the Federal Office of Administration	Grants and registers authorisations to read ID card data	Federal	personalausweisportal.de
Federal Office for Information Security (BSI)	Technical guidelines, including TR-03147 assurance levels for identity proofing	Federal	bsi.bund.de
Federal Network Agency (Bundesnetzagentur)	Supervisory body for trust services such as qualified electronic signatures	Federal	VDG § 2
Federal Commissioner for Data Protection (BfDI) and Länder data protection authorities	Data protection supervision of public bodies and of eID service providers	Federal and state	bfdi.bund.de
Local ID card authorities (Personalausweisbehörden)	Issue ID cards, capture fingerprints, reset or block the online function	Municipal, under state law	PAuswG § 9
European Commission	eIDAS implementing acts on wallets, person identification data and relying parties	Supranational	EUR-Lex

2 Licensing and authorisation

Reading ID card data: the authorisation certificate

Under § 21 of the Personalausweisgesetz (PAuswG, Identity Card Act), a service provider needs an authorisation (Berechtigung) to request data through the electronic identity function. The VfB grants it if the provider proves its identity, explains its interest in using the function, gives an assurance on data protection, and there is no indication of misuse. It lasts at most three years, is renewable, and covers only the data categories named in it (§ 18(5) PAuswG).

Separate authorisations exist for reading the card at a counter (§ 21a PAuswG) and for identification service providers that identify citizens on behalf of third parties (§ 21b PAuswG), which must also show technical and organisational measures that meet the deletion and purpose-limitation rules in § 19a. The VfB may ask the competent data protection authority whether it knows of any misuse (§ 29a of the Identity Card Ordinance, PAuswV). After approval, the provider contracts with a certificate provider for technical certificates, issued for 48 hours and renewed every 24 hours, and runs or buys an eID server.

Trust services and wallet relying parties

Providers of qualified electronic signatures, seals and time stamps are supervised by the Bundesnetzagentur under § 2 of the Vertrauensdienstegesetz (VDG, Trust Services Act). From 24 December 2026, any organisation that wants to rely on EU digital identity wallets must register in the Member State where it is established (Art. 5b eIDAS, applied through Implementing Regulation (EU) 2025/848) `Adopted, applies 24 Dec 2026`. Intermediaries acting for a relying party count as relying parties, and relying parties may not refuse pseudonyms where no law requires identification (Art. 5b(9) and (10) eIDAS). The Digital Identities Act (DIdG) passed by the Bundestag would make the Federal Office of Administration the German registration body `Bill, not enacted`; for the state wallet, testing each use case in the federal sandbox is a prerequisite for production use.

Requesting chip data without authorisation is fineable up to EUR 30,000 (§ 32 PAuswG).

3 Identity framework (AML rules do not apply)

The Geldwäschegesetz (GwG, Anti-Money Laundering Act) applies to businesses acting in the course of their trade or profession (§ 2(1) GwG). Authorities delivering public services are not on that list, so no customer due diligence or suspicious transaction reporting

regime applies to them as service providers. The narrow exception is public auctions: courts and authorities holding them must identify buyers and report to the Financial Intelligence Unit where cash payments of EUR 10,000 or more are made (§ 2(3) and (4) GwG).

Identity for public services is instead governed by four layers:

Identity documents

The PAuswG (German nationals), the eID-Karte-Gesetz (EU and EEA citizens) and § 78(5) of the Residence Act (AufenthG), all with the same online identity function.

Online Access Act

The Onlinezugangsgesetz (OZG) sets the citizen account and the identity means per assurance level.

Administrative procedure

§ 3a of the Administrative Procedure Act (VwVfG) and § 9a OZG say when an online declaration replaces the written form.

EU eIDAS Regulation

Regulation (EU) No 910/2014, amended by Regulation (EU) 2024/1183: assurance levels and the EU wallet.

The state eID is also a listed verification method for AML-obliged firms (§ 12(1) No 2 GwG).

4 Identity verification and onboarding

Assurance levels

§ 3(4) OZG ties each method to an eIDAS assurance level. For services needing at most "substantial", the citizen account accepts the tax administration's secure procedure under § 87a(6) of the Fiscal Code (the ELSTER certificate) or any eID scheme notified under Art. 6 eIDAS at "substantial" or above. For services needing "high", it accepts only the electronic identity function of the ID card, the eID card or the electronic residence permit, or a notified eID scheme at "high". Company accounts use ELSTER or a notified scheme at "substantial". Some Länder still run their own citizen accounts, which may stay in use for three years after the federal government announces in the Federal Law Gazette that automated migration to the central account is possible (§ 12(1) OZG); none had been made by October 2026. Länder are instead moving over by agreement; by April 2026, ten had switched to BundID.

The BSI's Technical Guideline TR-03147 (version 1.0.6 of 28 December 2021, still the current version) assesses identity-proofing procedures at the levels "normal", "substantial" and "high", designed to meet the eIDAS minimums for "low", "substantial" and "high".

How the online ID works

Card holders aged 16 or over (13 under the DIdG) can prove their identity electronically to public and private bodies (§ 18 PAuswG). The law also allows the function to be stored on a phone (§ 10a PAuswG), but the federal government describes the EU wallet as the first identification means at level "high" on mobile devices. Validity and the blocking feature are always sent, so the provider can check the blocking list. Optional data include names, date and place of birth, address, a service-specific pseudonym, and yes or no answers on age or residence. Data flow only after the provider presents a valid authorisation certificate and the holder, having seen who is asking and for what, enters the PIN.

Documents, copies and face matching

A card may be copied only by the holder or with the holder's consent, the copy must be clearly and permanently recognisable as a copy, and only the holder may pass a copy on to third parties (§ 20(2) PAuswG). Where a law allows it, public bodies may, with consent, read the chip photo to check identity and must delete it straight after (§ 20(3a) PAuswG). Fingerprints are stored on the chip (§ 5(9) PAuswG); carriers reading the card may not read biometric data (§ 20(4) PAuswG).

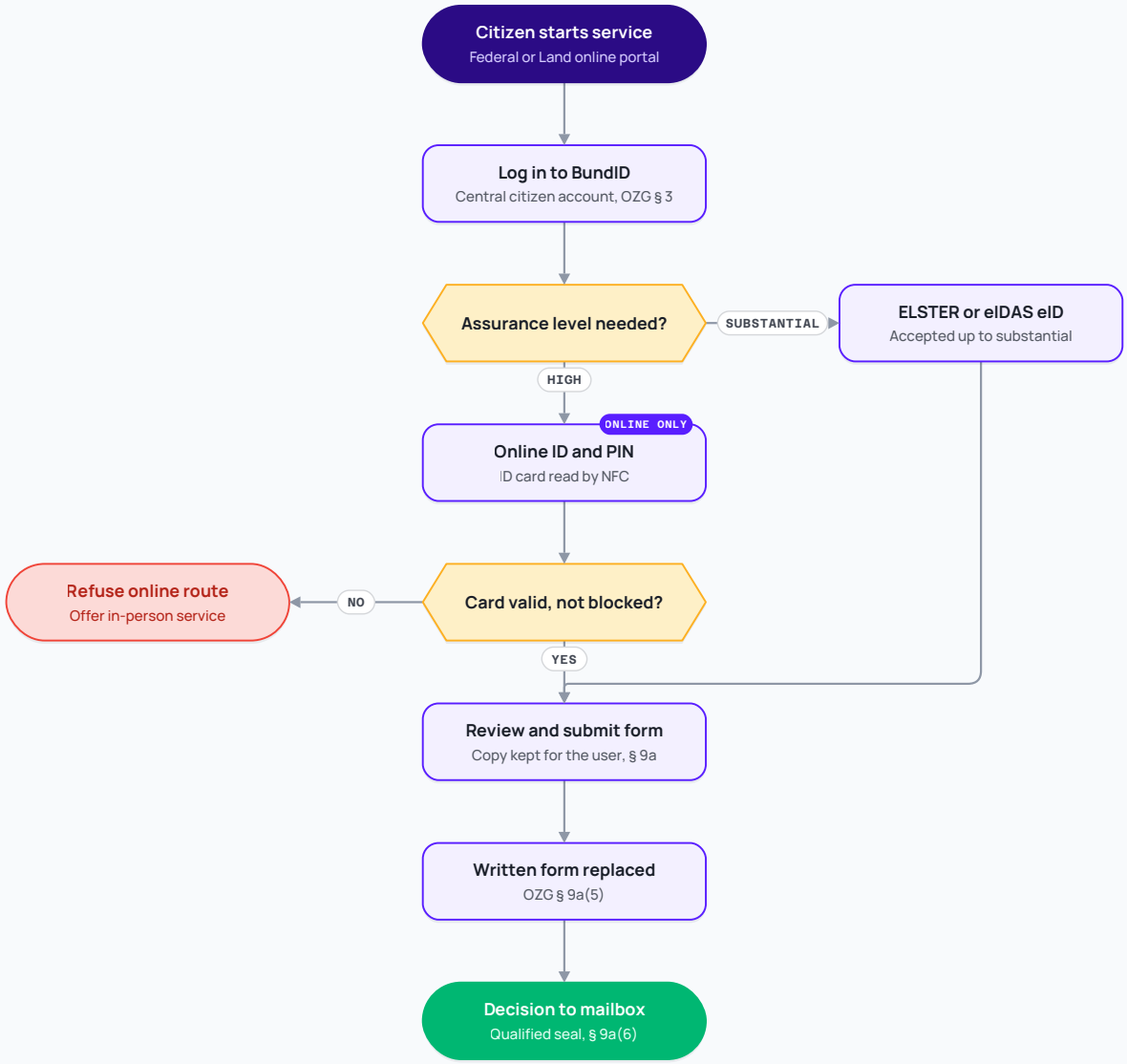


Figure 1. Online identification for a German public service through the BundID citizen account.

5 Digital channels: what's different

Bottom line: online, the law names the identity methods it accepts for each assurance level, and at "high" only state eIDs and notified EU schemes qualify; at the counter, the official checks the card and compares the photo.

Requirement	In person	Online / remote	Difference

Applying for the ID card	Applicant should appear in person; no representative	Not available; follow-up statements may be sent electronically	`Differs`
Proving identity for a service	Card shown, photo compared	Method set by assurance level (OZG § 3(4))	`Differs`
Accepted remote methods	Not applicable	State eID, ELSTER (up to substantial), notified eIDAS schemes	`Differs`
Replacing the written form	Handwritten signature	BundID identity proof plus portal form (§ 9a(5) OZG), eID in an official form, or QES (§ 3a VwVfG)	`Differs`
State authorisation to read chip data	Required (§ 21a), plus photo check and access number	Required (§ 21), plus holder's PIN	`Same`
Copies of the ID card	Only with consent, marked as copy	Same rule for scans and photos	`Same`
Recovering a forgotten PIN	New PIN set at the ID office	Reset letter ordered online, sent by post	`Differs`

A fixed list of remote methods

§ 3(4) OZG does not leave the choice of remote method to the authority. Video identification, document photo uploads and selfie matching are not among the methods it names for the citizen account, so on their own they cannot open a public service that requires "high". The BundID also offers password plus two-factor login where the competent authority allows it.

The online function is the bottleneck

Remote use depends on the PIN. The federal reset service, which posts a new PIN letter, was stopped at the end of 2023 and relaunched free of charge on 13 October 2026 for a limited period `Live, time-limited`; ID offices can also set a new PIN.

Pending changes

Under the DIdG as passed by the Bundestag, the EU wallet would become a third route into online public services next to the citizen account and the eID (§ 3(1) OZG as amended),

could be used wherever a rule requires the ID card's online function unless federal or state law excludes it, and could also be presented offline at a counter `Bill, not enacted`. The BundID already announces "d-you" as a login method from January 2027.

6 Data protection and biometrics

The General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG) apply in full; the ID card rules add sector limits on top. Service providers may store eID data to create or change a user account, or in an online form for as long as their business purpose requires (§ 19(5) and (6) PAuswG). Identification service providers must delete data as soon as the identification is complete and handed over (§ 19a PAuswG).

The data protection authorities' position paper on biometric analysis (3 April 2019, adopted against the votes of Bavaria and Baden-Württemberg) treats biometric identification as prohibited in principle under Art. 9(1) GDPR unless an Art. 9(2) exception applies, typically explicit consent. For public bodies, the face check against the chip photo rests on a statute instead (§ 20(3a) PAuswG). In its activity report for 2025, presented on 6 May 2026, the BfDI noted that, according to BSI studies, smartphone biometrics reach at best "substantial" and mostly only "normal", and argued that the EU wallet must support pseudonymous use where no law requires identification.

7 Sector-specific obligations

The EU digital identity wallet

Each Member State must provide at least one EU digital identity wallet within 24 months of the entry into force of the eIDAS implementing acts (Art. 5a(1) eIDAS), which BMDS gives as 24 December 2026. The state wallet "d-you" is due on 2 January 2027 with about 40 partner services; it is free and set up with an ID card or residence permit whose online function is active. Certified non-state wallets could be recognised about 12 months after launch (BMDS planning), once an ordinance under the DIdG allows it (§§ 6, 22). Since 10 October 2026, § 13 OZG lets BMDS approve wallet pilots that deviate from the citizen account rules for up to two years.

The Digital Identities Act (DIdG)

The Bundestag passed the DIdG on 15 October 2026 with committee amendments (printed papers 21/7408 and 21/8617). It needs Bundesrat consent and enters into force the day after promulgation `Bill, not enacted`. It would assign wallet provision to BMDS, relying

party registration to the Federal Office of Administration, certification to the BSI and supervision to the Bundesnetzagentur. Federal authorities would have to issue decisions as electronic attestations on request 12 months after promulgation. Users could exclude their photo from wallet identity data. The Act would also lower the eID age from 16 to 13, let people who were 70 or over when applying keep using an expired ID card as identification (but not its online function), and allow an electronic PIN reset after identification at level "high".

Mandatory acceptance

Public sector bodies that require electronic identification for an online service must also accept EU wallets (Art. 5f(1) eIDAS). Private relying parties, other than micro and small enterprises, that must use strong user authentication by law or contract (for example in banking, energy or health) must accept wallets at the user's voluntary request no later than 36 months after the implementing acts entered into force, that is by December 2027 (Art. 5f(2)) `Adopted, applies Dec 2027`.

8 Risk indicators and red flags

IDENTITY ABUSE INDICATORS IN PUBLIC-SERVICE IDENTIFICATION

- **Injection attacks**: deepfakes, replayed video or synthetic ID documents fed directly into the video stream of a remote check (BSI).
- **Edited application photos**: suspected manipulation lets the ID office order the photo to be taken on its premises (§ 9(4) PAuswG).
- **Blocked or expired eIDs**: a card on the blocking list after loss, theft or death must not be accepted (§ 10 PAuswG).
- **PIN known to others**: use of the online ID by anyone other than the holder is unlawful and a fineable offence (§ 18(2), § 32(1) No 5 PAuswG).
- **Forwarded ID copies**: copies passed on by anyone but the holder, or unmarked scans sent by unencrypted email (§ 20(2) PAuswG; BMI guidance).
- **Weak account recovery**: hotline and portal flows that let a third party take over an account or eSIM profile (BfDI, 2025).
- **Over-trusting device biometrics**: phone face or fingerprint unlock used as if it met level "high" (BfDI, citing BSI).

9 Enforcement and penalties

- **Identity card law**: up to EUR 30,000 for requesting data without authorisation, using a revoked certificate or using another person's online ID, and up to EUR 3,000 for offences such as passing on a copy of someone's ID card (§ 32(3) PAuswG). The VfB can also withdraw the authorisation at a data protection authority's request (§ 21(4)).
- **Data protection, private firms**: GDPR fines under Art. 83(4) and (5), in two tiers of up to EUR 10 million or 2% and up to EUR 20 million or 4% of worldwide annual turnover, whichever is higher.
- **Data protection, public bodies**: no administrative fines may be imposed on federal authorities and other public bodies (§ 43(3) BDSG); supervisors use warnings and orders instead.

In its 2025 activity report, the BfDI described a EUR 30 million fine on a telecommunications provider whose combined portal and hotline authentication could let third parties take over another person's eSIM profile and phone number (Art. 32 GDPR).

10 Recent changes and what to watch

- **10 July 2027**: the EU Anti-Money Laundering Regulation applies; obliged entities may verify customers with eID means at level "substantial" or "high" under eIDAS (Art. 22(6) AMLR) `Adopted, applies 10 Jul 2027`.
- **2 January 2027**: planned launch of the state wallet "d-you" and its availability as a BundID login `Planned launch`.
- **24 December 2026**: relying party registration rules for EU wallets apply (Implementing Regulation (EU) 2025/848) `Adopted, applies 24 Dec 2026`. Register before requesting wallet data.
- **15 October 2026**: Bundestag passes the Digital Identities Act; now before the Bundesrat (printed paper 618/26; committee 4 November, plenary 20 November 2026) `Bill, not enacted`.
- **13 October 2026**: PIN reset letter service relaunched free of charge for a limited period `Live, time-limited`.
- **10 October 2026**: § 13 OZG allows time-limited wallet pilot exemptions from citizen account rules `In force`. Pilots must still set up wallets at level "high".
- **30 September 2026**: BSI consultation on its draft evaluation guidance for injection attack detection (version 0.3, 22 July 2026) closed `Consultation closed, draft`.

- **1 May 2025**: ID card photos must be taken digitally by an authority or a photo service provider and transmitted securely `In force`.

11 What this means for identity verification

- **Design for the state eID first.** For public services at "high", the ID card's online function (and the eID card and electronic residence permit) is the default; build NFC reading through an authorised eID server rather than document scanning.
- **Map each journey to an assurance level.** The level decides the accepted methods, and request only the data the service needs, using age checks or the pseudonymous identifier where possible.
- **Plan for wallets on two clocks.** Register as a relying party from 24 December 2026; regulated firms using strong authentication must accept wallets by December 2027, and AML-obliged firms can rely on eIDAS eID means from July 2027.
- **Treat copies and photos as restricted data.** Copy only with consent, mark copies and delete chip photos after a face check.
- **Prepare for remote proofing assessments.** Video and selfie-based methods outside the eID route are measured against BSI TR-03147, including injection attack detection.

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 reading of electronic ID chips, for journeys outside the state eID route.
- Biometric liveness and face match for remote identity proofing, with configurable checks as BSI injection-attack guidance develops.
- Age verification and data-minimising checks that request only the attributes a service needs.
- No-code workflow builder to route each journey by assurance level, with an audit trail for every check.
- Cloud, on-premises or hybrid deployment for public-sector data residency requirements.

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

- **Gesetz über Personalausweise und den elektronischen Identitätsnachweis (PAuswG) [Identity Card Act]**, as last amended by Art. 3 of the Act of 16 July 2026 (BGBl. 2026 I Nr. 213), §§ 4, 5, 9, 10, 10a, 18, 18a, 19, 19a, 20, 21, 21a, 21b, 27, 32, gesetze-im-internet.de
- **Onlinezugangsgesetz (OZG) [Online Access Act]**, as amended by the Act of 19 July 2024 (BGBl. 2024 I Nr. 245) and Art. 3 of the Act of 6 October 2026 (BGBl. 2026 I Nr. 289), §§ 2, 3, 9a, 12, 13, gesetze-im-internet.de

- **Gesetz zur Stärkung des Innovations- und Wirtschaftsstandorts Deutschland durch Erprobungsfreiräume**, 6 October 2026, BGBl. 2026 I Nr. 289 (published 9 October 2026), Art. 3, recht.bund.de
- **eID-Karte-Gesetz [eID Card Act]**, §§ 1, 12, gesetze-im-internet.de
- **Aufenthaltsgesetz (AufenthG) [Residence Act]**, § 78(5) to (7), gesetze-im-internet.de
- **Verwaltungsverfahrensgesetz (VwVfG) [Administrative Procedure Act]**, § 3a, gesetze-im-internet.de
- **Vertrauensdienstegesetz (VDG) [Trust Services Act]**, § 2, gesetze-im-internet.de
- **Geldwäschegesetz (GwG) [Anti-Money Laundering Act]**, as last amended by Art. 12(4) of the Act of 29 June 2026 (BGBl. 2026 I Nr. 197), §§ 2, 12, 44, gesetze-im-internet.de
- **Regulation (EU) 2016/679 (General Data Protection Regulation)**, Art. 83, eur-lex.europa.eu
- **Bundesdatenschutzgesetz (BDSG) [Federal Data Protection Act]**, § 43, gesetze-im-internet.de
- **Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 (eIDAS)**, 11 April 2024, Arts. 5a, 5b, 5f, eur-lex.europa.eu
- **Commission Implementing Regulation (EU) 2024/2977** on person identification data and electronic attestations of attributes, OJ L 4.12.2024, eur-lex.europa.eu
- **Commission Implementing Regulation (EU) 2025/848** on the registration of wallet-relying parties, 6 May 2025, Art. 11, eur-lex.europa.eu
- **Digitale Identitätengesetz (DIdG) [Digital Identities Act], legislative procedure**, DIP, status "Verabschiedet" (2nd and 3rd reading 15 October 2026), dip.bundestag.de; government bill, BT-Drucksache 21/7408, 29 July 2026, Art. 1 §§ 2, 10, 15, 16, 20, Arts. 2, 11, 12, 14, bundestag.de; committee recommendation and report, BT-Drucksache 21/8617, 14 October 2026 (advance version), bundestag.de
- **Antwort der Bundesregierung, "Vorschlag 31202 der Verbändeabfrage zur Bürokratieentlastung" [Federal Government answer]**, BT-Drucksache 21/5367, 13 April 2026, answer to question 8, bundestag.de
- **Bundesrat, Beratungsvorgang 618/26 (DIdG as passed by the Bundestag)**, received 30 October 2026, bundesrat.de; Ausschuss für Digitales und Staatsmodernisierung, 10th meeting, 4 November 2026, agenda, bundesrat.de
- **Deutscher Bundestag, Plenarprotokoll 21/102**, 15 October 2026, pp. 12852C-12859D (adoption in the committee version), bundestag.de
- **BSI, "Handlungsleitfaden zur Anbindung der EUDI-Wallet"**, version 0.6, 3 December 2025, bsi.bund.de
- **Stellungnahme des Bundesrates zum DIdG [Bundesrat opinion]**, BR-Drucksache 322/26 (Beschluss), 10 July 2026, points 6 and 7, bundesrat.de
- **Antwort der Bundesregierung, "Umsetzungsstand, Projektsteuerung und technische Ausgestaltung der deutschen EU Digital Identity Wallet" [Federal Government answer]**, BT-Drucksache 21/7319, 21 July 2026, bundestag.de

- **Organisationserlass des Bundeskanzlers [Organisational decree of the Federal Chancellor]**, 6 May 2025, BGBl. 2025 I Nr. 131, section XII, recht.bund.de
- **Personalausweisverordnung (PAuswV) [Identity Card Ordinance]**, § 29a, gesetze-im-internet.de
- **Regulation (EU) 2024/1624 (Anti-Money Laundering Regulation)**, Art. 22(6) and Art. 90, eur-lex.europa.eu
- **EUDI-Wallet project, FAQ** (BMDS), eudi-wallet.gov.de
- **Personalausweisportal (BMI), FAQ "Diensteanbieter werden"**, personalausweisportal.de
- **BMDS, "EUDI-Wallet d-you"**, bmds.bund.de
- **BMDS press release 53/2026, "d-you"**, 9 September 2026, bmds.bund.de
- **BMDS press release 24/2026, "Kabinett beschließt Gesetz für digitale Identitäten"**, 20 May 2026, bmds.bund.de
- **BMDS press release 67/2026, "Online-Ausweis: Neue PIN ohne Gang zum Bürgeramt"**, 13 October 2026, bmds.bund.de
- **BMDS, "BundID"**, bmds.bund.de
- **Personalausweisportal (BMI), "So werden Sie Diensteanbieter"**, personalausweisportal.de
- **Personalausweisportal (BMI), "Was Sie beim Ausweisen im Alltag wissen und beachten sollten"**, 19 September 2025, personalausweisportal.de
- **BSI, Technische Richtlinie TR-03147, Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen [assurance level assessment of identity proofing procedures]**, version 1.0.6, 28 December 2021, bsi.bund.de
- **BSI, "Evaluation Guidance Injection Attacks"**, draft version 0.3, 22 July 2026, bsi.bund.de
- **BSI, "TR-03147 Assurance Level Assessment of Procedures for Identity Verification of Natural Persons"**, page updated 31 July 2026, incl. consultation on injection attack detection, bsi.bund.de
- **BfDI, 34. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit 2025 [34th activity report]**, presented 6 May 2026, sections 4.2 and 7.1, bfdi.bund.de; press release 6/2026, bfdi.bund.de
- **Datenschutzkonferenz, "Positionspapier zur biometrischen Analyse"**, version 1.0, 3 April 2019, datenschutzkonferenz-online.de