



Identomat

COMPLIANCE GUIDE

Healthcare Compliance in Bulgaria

COUNTRY **Bulgaria**

INDUSTRY **Healthcare**

LAST UPDATED **21 October 2026**

KEY REGULATORS **Ministry of Health · Executive Agency for Medical Supervision · Bulgarian Drug Agency**

Key takeaways

- Hospitals, clinics, telehealth services and pharmacies are not covered by Bulgaria's anti-money laundering law. Their identity duties come from health legislation: patients show an identity document, and remote care needs reliable electronic identification.
- Remote medical care (telemedicine) has been lawful since 1 April 2025, but only a medical facility set up under Bulgarian law may provide it. A May 2026 ordinance forbids remote care when the patient's identity cannot be established reliably.
- Prescription-only medicines may not be sold online. Non-prescription medicines may be sold online only by a licensed pharmacy or drugstore showing the EU common logo.
- Every consultation, including a remote one, must be recorded in the national health information system as a document signed with a qualified electronic signature (the EU's highest-trust e-signature). Patients open their records with high-assurance electronic identity or a state app activated in person.
- Health data is a special category under EU data protection law, and Bulgarian law lets a business copy an identity document only where a statute allows it. EU rules giving patients new digital access rights apply from March 2027, with core rights from March 2029.

Bulgaria is open to digital health. Telemedicine has had its own legal basis since 2025, the national health information system is mandatory for every provider, and patients reach their electronic health records with electronic identity. The market is, however, closed to anyone who is not a Bulgarian-registered medical facility: a platform cannot deliver care in its own name.

The Ministry of Health sets the rules and runs the national health information system; the Executive Agency for Medical Supervision registers outpatient facilities and supervises remote care; the Bulgarian Drug Agency licenses pharmacies and lists online sellers of medicines; the National Health Insurance Fund pays for insured care; and the Commission for Personal Data Protection supervises health data.

The biggest obstacle for a new entrant is structural: telehealth, e-prescribing and online pharmacy all sit inside the licensed facility or pharmacy, and the prohibition on online sale of prescription medicines rules out the full remote prescribe-and-deliver model.

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

Regulator	Remit	Level	Official site
Ministry of Health	Health policy and ordinances; hospital permits; administers the National Health Information System (NHIS)	National	mh.government.bg
Executive Agency for Medical Supervision	Registration of outpatient facilities and hospices; control of medical facilities, including remote care	National	iamn.bg
Bulgarian Drug Agency	Pharmacy permits; register and public list of online sellers of medicines	National	bda.bg
National Health Insurance Fund	Contracts with providers for insured care; reimbursement of medicines	National	nhif.bg
Commission for Personal Data Protection	Supervision of the General Data Protection Regulation (GDPR) and the Personal Data Protection Act	National	cpdp.bg
Bulgarian Medical Association; Bulgarian Pharmaceutical Union	Statutory professional bodies keeping registers of doctors and pharmacists	National	blsbg.com ; bphu.bg

European Union

Directly applicable
regulations: GDPR, the
European Health Data Space
Regulation, eIDAS

Supranational

eur-lex.europa.eu

Regional health inspectorates and the National Revenue Agency also play a role: the inspectorates act locally for the Ministry, and the Agency supplies the health insurance status that providers must check before treating insured patients.

2 Licensing and authorisation

Under the Medical Treatment Facilities Act (Закон за лечебните заведения, MTFA), outpatient facilities and hospices are registered by the Executive Director of the Executive Agency for Medical Supervision (Articles 39 and 40). Hospitals, dialysis centres and similar facilities need a permit from the Minister of Health (Article 46), and for hospitals and comprehensive cancer centres only after a Council of Ministers decision. Practising outpatient care without registration carries a fine of 2,000 to 5,000 leva and, on a repeat breach, loss of the right to practise for three months to one year (Article 115(2)).

Telemedicine needs no separate licence

Article 6b MTFA **In force since 1 Apr 2025** lets medical facilities and their specialists provide care at a distance. Ordinance No. H-5 of 28 April 2026 on remote medical care confirms that only facilities established under the MTFA may do so, and excludes transfusion haematology centres and tissue banks (Article 4). Facilities may pool resources in remote-care centres by written contract, which must allocate data protection duties as joint controllers (Article 5). A technology company can supply the platform, but the facility delivers and answers for the care.

Pharmacies and online sale

A permit for retail sale of medicines in a pharmacy is issued by the Executive Director of the Bulgarian Drug Agency (Article 228, Medicinal Products in Human Medicine Act, Закон за лекарствените продукти в хуманната медицина). Online sale is an extension of that permit, not a licence of its own (see section 5). Providers who want public funding sign contracts with the National Health Insurance Fund under the Health Insurance Act.

Identity framework (AML rules do not apply)

The Measures Against Money Laundering Act (Закон за мерките срещу изпирането на пари, as amended up to State Gazette No. 51 of 2026) lists its obliged entities in Article 4: banks, payment and e-money institutions, insurers, investment firms, gambling operators, crypto-asset service providers and certain professions and traders. Medical facilities, telehealth services and pharmacies are not on the list, so customer due diligence, beneficial ownership checks and suspicious transaction reporting do not apply to them as healthcare providers.

Patient identity is governed instead by health legislation:

Identity document at the point of care

Insured patients must present an identity document, and providers must check the patient's health insurance status against National Revenue Agency data (Article 50, Health Insurance Act).

State registers as the reference

The NHIS receives civil registration data from the national population database and identity document validity from the national register of Bulgarian identity documents "for the purposes of identifying natural persons" (Article 28g(5), Health Act).

Patient identifiers

Each electronic health file carries the patient's names and personal number (ЕГН or ЛНЧ); foreigners without one are identified by date of birth, social security number or identity document number (Article 15(3), Ordinance No. H-6 of 2022).

Informed consent

Medical activities need the patient's informed consent; minors aged 14 to 18 also need a parent's consent, except that from 16 a patient may consent alone to consultations and preventive examinations (Article 87, Health Act).

Identity verification and onboarding

In person, identification rests on the identity document shown at the counter. Online, Ordinance No. H-5 turns identity into a precondition for treatment: remote care is provided through technology that ensures "reliable identification of the participants" (Article 6(1)(3)), and it may not be provided at all when the identity of the patient or of the person requesting the service cannot be established reliably (Article 7(1)(4)). The ordinance does

not name a method or an assurance level, so the facility chooses one and must be able to justify it to the Executive Agency for Medical Supervision.

- **Request form.** The patient applies through an electronic form that must contain identification data, contact details, the health problem, consent to remote care and data processing, and consent to any audio or video recording (Article 18(2)). The facility must keep the request traceable (Article 18(5)).
- **Clinician side.** The record of a remote consultation is signed with a qualified electronic signature or another recognised method of electronic identification (Article 20(1)).
- **Patient access to records.** Patients reach their electronic health file with an electronic identification means under the Electronic Identification Act, an eIDAS-notified means at assurance level "high", a "high" means from a qualified trust service with national coverage, or the state eZdrave app, activated in person on presentation of an identity document (Articles 23 and 23a, Ordinance No. H-6, as amended in State Gazette No. 57 of 2024).
- **Consent to a provider's access.** A patient can authorise a facility to see the file by qualified electronic signature, a signature pad or a one-time code sent by the NHIS to the patient's phone. The pad and code routes require a prior written agreement signed at the facility (Article 25(2), Ordinance No. H-6).

No Bulgarian health rule specifies liveness or presentation-attack standards for patient onboarding. Document-and-selfie checks are not prohibited, but they meet the data protection limits in section 6.

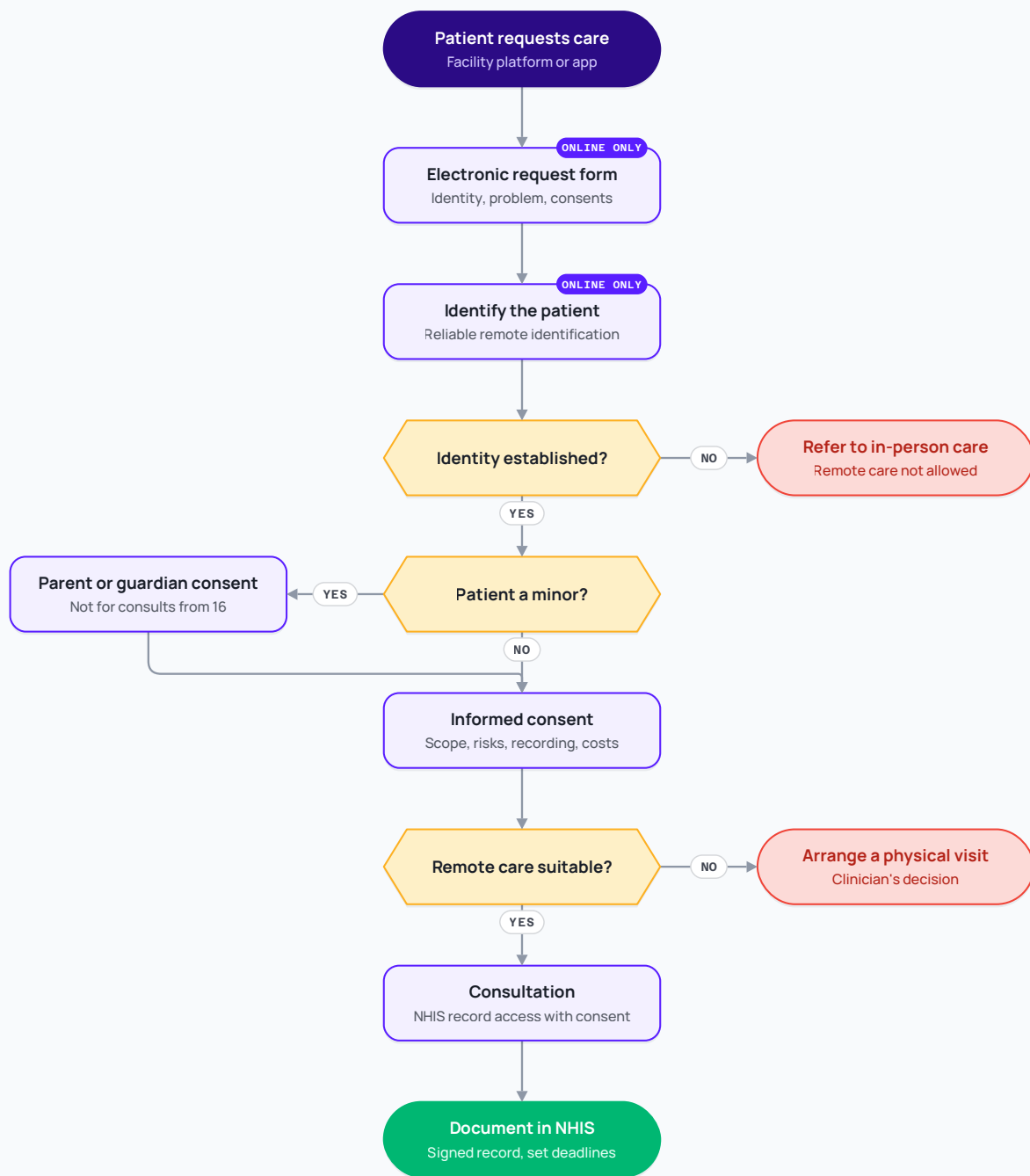


Figure 1. Remote consultation flow for a Bulgarian medical facility under Ordinance No. H-5 of 2026.

Bottom line: online, identity becomes a gate rather than a formality. A remote consultation cannot go ahead unless the patient is identified reliably, and prescription-only medicines cannot be sold online at all.

Requirement	In person	Online / remote	Difference
Who may provide care	Registered or permitted medical facility	Same facilities, except transfusion centres and tissue banks	Differs
Patient identification	Identity document and insurance status check	Reliable electronic identification; no care if identity is not established	Differs
Informed consent	Health Act rules; written for high-risk procedures	Ten additional disclosures, given before the service	Differs
Recording the encounter	No specific rule	Audio or video only with prior written or electronic consent	Differs
Documentation	Signed electronic record in the NHIS	Same, by 16:00 next working day (30 minutes for urgent consults)	Differs
Access to the patient's record	Explicit consent of the patient	Explicit consent, limited to what the consultation needs	Same
Prescription-only medicines	Dispensed in a pharmacy	Online sale prohibited	Differs
Non-prescription medicines	Pharmacy or drugstore	Only a permitted pharmacy or drugstore with the EU common logo	Differs
Data protection	GDPR Article 9(2) (h)	Also an impact assessment and an online privacy notice	Differs

Telemedicine consent and timing

Before remote care, the patient must be told its scope, data protection measures, alternatives, risks, limitations, the names and specialties of the clinicians, the right to stop at any time and any cost (Article 6b(5) and (6) MTFA). Ordinance No. H-5 adds documentation deadlines: planned care by 16:00 on the next working day, complex cases within two working days, urgent consultations within 30 minutes or, for complex imaging, 120 minutes (Article 17(2)). Childbirth may not be managed and death may not be established remotely, and dental care is limited to consultations between dentists and interpretation of images (Article 7).

Online pharmacy

Article 234(4) of the Medicinal Products in Human Medicine Act prohibits internet sale of prescription-only medicines. Non-prescription medicines may be sold online only by a pharmacy or drugstore holding the relevant permit, and the website must display the EU common logo (Article 234(6) and (7)). The Bulgarian Drug Agency publishes the list of online sellers and their web addresses (Article 234a). Unlawful internet trade in medicines carries a fine of 5,000 to 10,000 leva (Article 287b).

Cross-border telehealth

For cross-border healthcare, telemedicine services are treated as provided in the member state where the provider is established (Health Insurance Act, Additional Provisions, § 1b, point 4). A foreign platform serving Bulgarian patients without a Bulgarian facility is therefore outside the domestic telemedicine regime.

What is changing

The European Health Data Space Regulation, Regulation (EU) 2025/327

Adopted, applies from 26 Mar 2027, gives patients the right to identify themselves to health data access services with any eIDAS-recognised electronic identification means (Article 16).

6 Data protection and biometrics

GDPR applies directly and treats health data and biometric data used to identify a person as special categories (Article 9(1)); care providers process health data on the basis of

Article 9(2)(h). The Personal Data Protection Act (Закон за защита на личните данни) adds three rules that bite on digital onboarding:

- **Copies of identity documents.** A controller may copy an identity document, driving licence or residence document only where a law provides for it (Article 25g). Health legislation requires patients to present an identity document, not to hand over a copy, so capturing and keeping a document image needs a statutory basis. A biometric face match also needs its own Article 9 condition, usually explicit consent.
- **Children online.** Consent-based processing for a child under 14 using an information society service is lawful only with consent from a parent or guardian (Article 25v).
- **Large-scale processing.** Controllers processing data on a large scale must adopt internal rules (Article 25d).

Ordinance No. H-5 requires every remote-care facility to carry out a data protection impact assessment (Article 29), to publish a privacy notice on its website and give it to the patient when the service is requested (Article 30), and to process only the data the consultation needs (Article 28(2)). Recording consent must state purpose, storage period and who has access (Article 19(2)). In the NHIS, a deceased person's electronic health file is kept for 50 years after death (Article 17(2), Ordinance No. H-6).

7 Sector-specific obligations

The mandatory electronic health record

Since 8 October 2024, medical and non-medical specialists must create an electronic health record for every activity, and health documentation is sent to the NHIS as an electronic document signed with a qualified electronic signature (Article 28g(3a), Health Act). Facilities may not charge patients for this (Article 28g(3c)), paper copies may not be required except for technical reasons or at the patient's request (Article 28g(9)), and the patient must confirm each examination in the NHIS by one of the approved signing methods (Article 14(4), Ordinance No. H-6). Third parties, including insurers, reach the record only with the patient's explicit written consent (Article 28d(2), Health Act).

Electronic prescriptions

Prescriptions are part of each patient's electronic health file (Article 15(3), Ordinance No. H-6), and the NHIS checks health insurance status with the National Revenue Agency in real time when an electronic prescription is issued and dispensed (Article 29(5)). Since 1 September 2024 a partly dispensed electronic prescription may be completed at the same

or another contracted pharmacy within two working days (amendment to Ordinance No. 4 of 2009, State Gazette No. 68 of 2024).

Technology and vendor controls for remote care

Software with a medical purpose used in remote care must carry valid CE marking (Article 25(2), Ordinance No. H-5); systems must meet the NHIS cybersecurity requirements (Article 24(2)); contracts with external platform providers must secure the availability and integrity of health data (Article 27(3)); and clinical decision support tools require transparency and human control (Article 24(4)). The use of such tools must be noted in the medical record (Article 20(4)).

8

Risk indicators and red flags

IDENTITY AND ACCESS ABUSE IN DIGITAL HEALTH

- **Unverifiable remote patient:** the patient's identity cannot be established reliably, which bars remote care outright.
- **Mismatch with state registers:** personal number or document data that the population register or identity document register does not confirm.
- **Borrowed insurance:** a person seeking insured care with another person's identity or an unverified insurance status.
- **Proxy requests:** an adult requesting care or record access for someone else without a written authorisation or parental status.
- **One-time codes to an unregistered phone:** consent codes sent to a number not tied to a prior signed agreement at the facility.
- **Prescription medicines ordered online:** any website offering prescription-only medicines, or a seller absent from the Bulgarian Drug Agency list.
- **Unconsented recording:** audio or video of a consultation captured without prior written or electronic consent.

9

Enforcement and penalties

The Executive Agency for Medical Supervision controls facilities and specialists providing remote care (Article 21, Ordinance No. H-5). Penalties under the MTFA are fixed per breach

and quoted here in leva, as in the consolidated text published by the Ministry of Health in August 2026:

Breach	Individual	Legal entity	Provision
Outpatient care in breach of the MTFA or its ordinances	1,000 to 3,000 leva	2,000 to 5,000 leva	MTFA Article 115(1), (3)
Outpatient care without registration	2,000 to 5,000 leva; on repeat, loss of the right to practise for 3 to 12 months	2,000 to 5,000 leva	MTFA Article 115(2), (3)
Hospital care in breach of the MTFA	1,000 to 5,000 leva	8,000 to 20,000 leva	MTFA Article 116
Breach of approved health information standards	500 to 1,000 leva	500 to 1,000 leva	MTFA Article 116v
Unlawful internet trade in medicines	5,000 to 10,000 leva		Medicinal Products Act Article 287b

For data protection breaches, GDPR fines are set by the Commission for Personal Data Protection on a percentage-of-turnover basis: up to EUR 10 million or 2% of worldwide annual turnover for controller obligations such as security and impact assessments, and up to EUR 20 million or 4% for breaches of the core principles and of Article 9, whichever is higher (Article 83(4) and (5)).

10 Recent changes and what to watch

- **24 Dec 2027** *Adopted, applies 24 Dec 2027* : private service providers, including in health, that are required by law to use strong user authentication must accept European Digital Identity Wallets at the user’s request (Article 5f(2), eIDAS as amended by Regulation (EU) 2024/1183).
- **26 Mar 2027** *Adopted, applies from 26 Mar 2027* : the European Health Data Space Regulation starts to apply; patient access rights apply from 26 March 2029 for the first priority data categories.

- **1 Nov 2026** **Adopted, effective 1 Nov 2026** : medical commissions of the National Social Security Institute gain access to electronic health records, only with the person's explicit written consent (Health Act Article 28d, State Gazette No. 68 of 2026).
- **5 May 2026** **In force** : Ordinance No. H-5 on remote medical care published in State Gazette No. 41, setting identification, consent, documentation and technology rules.
- **1 Jan 2026** **In force** : an appointment scheduling system within the NHIS that clinicians may use free of charge on a voluntary basis (Health Act Article 28z).
- **1 Apr 2025** **In force** : Article 6b MTFA makes remote medical care lawful for registered facilities.
- **8 Oct 2024** **In force** : mandatory electronic health record for every activity, signed with a qualified electronic signature (State Gazette No. 85 of 2024).

11 What this means for identity verification

- **Identity is a clinical precondition.** A remote-care flow needs a verification step that can say "not established" and route the patient to in-person care.
- **Lean on state identity.** High-assurance national electronic identification, eIDAS-notified means and qualified signatures are the methods the NHIS already recognises; the European Digital Identity Wallet will join them.
- **Document capture needs a legal basis.** Because a copy of an identity document may be kept only where a law provides, check data minimisation before storing document images, and record the legal basis and Article 9 condition for any face match.
- **Age and guardianship.** Capture date of birth (derivable from the ЕГН) to apply the 14 and 16 consent thresholds, and verify a parent's or guardian's link to the child.
- **Foreign patients.** Support identifiers other than the ЕГН/ЛНЧ, such as date of birth with a passport number.
- **Evidence.** Keep a traceable log of the request, identification result, consents and any recording consent; NHIS records of deceased patients are kept for 50 years after death.

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:

- Reliable remote patient identification before a teleconsultation, with ID document capture and verification (including NFC), face match and biometric liveness.
- Age verification to apply the parental consent thresholds for patients under 14 and under 16.
- Phone and email verification to support consent and contact steps in the remote-care request form.
- Configurable no-code workflows that route patients whose identity cannot be established to in-person care, with an audit trail of each check.
- Cloud, on-premises or hybrid deployment to keep patient identity data where the facility's data protection assessment requires.

[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 за лечебните заведения [Medical Treatment Facilities Act]**, consolidated text, Articles 6b, 10, 39, 40, 46, 115, 116, 116v, Ministry of Health, published 24 August 2026, mh.government.bg
- **Закон за здравето [Health Act]**, consolidated text, Articles 28d, 28g, 28z, 87, Ministry of Health, published 24 August 2026, mh.government.bg
- **Закон за здравното осигуряване [Health Insurance Act]**, consolidated text, Article 50 and Additional Provisions § 1b, Ministry of Health, published 24 August 2026, mh.government.bg

- Закон за лекарствените продукти в хуманната медицина [Medicinal Products in Human Medicine Act], consolidated text, Articles 228, 234, 234a, 287b, Ministry of Health, published 24 August 2026, mh.government.bg
- Наредба № Н-5 от 28 април 2026 г. за оказване на медицинска помощ от разстояние [Ordinance No. H-5 on remote medical care], State Gazette No. 41 of 5 May 2026, mh.government.bg
- Наредба № Н-6 от 21 декември 2022 г. за функционирането на Националната здравноинформационна система [Ordinance No. H-6 on the National Health Information System], State Gazette No. 103 of 2022, mh.government.bg; amended State Gazette No. 57 of 5 July 2024 (Articles 23, 23a), mh.government.bg
- Наредба за изменение и допълнение на Наредба № 4 от 2009 г. [Amendment to Ordinance No. 4 of 2009 on prescribing and dispensing medicines], State Gazette No. 68 of 13 August 2024, in force 1 September 2024, mh.government.bg
- State Gazette search results for Ordinances H-5, H-6 and No. 4, dv.parliament.bg
- Закон за мерките срещу изпирането на пари [Measures Against Money Laundering Act], consolidated to State Gazette No. 51 of 2026, Article 4, Financial Supervision Commission, fsc.bg
- Закон за защита на личните данни [Personal Data Protection Act], Articles 25d, 25g, 25v, Commission for Personal Data Protection, cpdp.bg
- Regulation (EU) 2016/679 (GDPR), Articles 9 and 83, eur-lex.europa.eu
- Regulation (EU) 2025/327 on the European Health Data Space, Articles 16 and 105, eur-lex.europa.eu
- Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 (eIDAS), Articles 5a and 5f, eur-lex.europa.eu; Commission Implementing Regulation (EU) 2024/2977, in force 24 December 2024, eur-lex.europa.eu