EUROPEAN COMPLIANCE SUITE

EU AI Act Compliance Evidence Templates

THE EU DIGITAL REGULATORY MAP

Sixty-plus laws, frameworks and standards live in the European Union today that can touch a digital product — with, for each, a one-line note on who or what it applies to. A starting map for working out which ones reach you.

Document	Reference map — EU digital regulation, frameworks and standards
Edition	July 2026
Publisher	European Compliance Suite (a trading name of EuroGRC OÜ)
How to use it	Scan the applicability column, mark what plausibly reaches your product, then get advice on the ones that do
Coverage	Binding EU law in force or in application, plus the principal voluntary standards and codes used to demonstrate compliance

This map is a high-level orientation tool, not legal advice and not a compliance checklist. Whether any instrument applies to a given product turns on the specific facts, and many of these laws phase in over several years, carry exemptions, or are transposed differently across Member States. Applicability descriptions are deliberately compressed to a single line and omit exceptions. Verify the current text and your own position with a qualified adviser before relying on anything here. Instruments are identified by their common names; several have been amended since first adoption.

How to read this map

(1) The European Union now regulates digital products through dozens of overlapping instruments — some horizontal (reaching almost every product), some sector-specific, some voluntary standards that provide the practical route to showing compliance. For anyone building or selling a digital product, the first problem is not how to comply; it is working out which of these even apply. This map exists to make that first problem tractable. It lists the instruments by theme, and for each gives a single line on who or what it applies to, so you can scan, mark what plausibly reaches your product, and narrow dozens of possibilities to the handful that actually matter for you.

(2) The map is intentionally broad and intentionally shallow. Breadth, because the risk for most organisations is not misreading a law they know about but never noticing one that applies. Shallow, because a one-line note cannot capture thresholds, exemptions or phase-in dates — and pretending otherwise would be worse than useless. Treat a match here as a prompt to look properly, not as a finding. Where a theme below is one European Compliance Suite has built detailed templates for, that is noted; the rest of the map is here because you should know the instrument exists.

1. Artificial intelligence

Framework	Who / what it applies to
AI Act — Reg (EU) 2024/1689	Providers, deployers, importers and distributors of AI systems, and providers of general-purpose AI models, placing them on or using them in the EU market; obligations scale with risk tier.
ISO/IEC 42001	Organisations wanting a certifiable AI management system — the practical governance backbone many use to operationalise AI Act duties.
ISO/IEC 23894	Teams needing a structured method for AI-specific risk management across the model lifecycle.
ISO/IEC 24028 / TR series	Developers addressing trustworthiness, robustness and transparency of AI systems in technical terms.
NIST AI Risk Management Framework	A voluntary, widely-referenced framework for AI risk — useful as best practice, not an EU legal requirement.

2. Data protection and privacy

Framework	Who / what it applies to
GDPR — Reg (EU) 2016/679	Any organisation processing personal data of people in the EU, wherever the organisation is established.
ePrivacy Directive — 2002/58/EC	Anyone using cookies or similar technologies, sending electronic marketing, or handling electronic-communications metadata.
Data Protection LE Directive — 2016/680	Authorities (and their processors) handling personal data for law-enforcement purposes.
Reg (EU) 2018/1725	EU institutions, bodies and agencies processing personal data — relevant to those who supply them.
ISO/IEC 27701	Organisations extending an information-security system to privacy information management, often to evidence GDPR accountability.
EU–US Data Privacy Framework	Organisations transferring EU personal data to certified US recipients under the current adequacy arrangement.

3. Data, data sharing and the data economy

Framework	Who / what it applies to
Data Act — Reg (EU) 2023/2854	Makers of connected products and related services, and cloud providers — governs access to co-generated data and switching between services.
Data Governance Act — Reg (EU) 2022/868	Data intermediaries, providers of data-altruism services, and public bodies making protected data available for re-use.
Open Data Directive — 2019/1024	Public-sector bodies and public undertakings making their data available for re-use.
Free Flow of Non-Personal Data — Reg (EU) 2018/1807	Providers and users of data-processing services — bars unjustified data-localisation requirements for non-personal data.
European Health Data Space — Reg (EU) 2025/327	Makers of electronic health record systems and holders of health data — governs primary use and controlled secondary re-use of health data.

4. Cybersecurity

Framework	Who / what it applies to
Cyber Resilience Act — Reg (EU) 2024/2847	Manufacturers, importers and distributors of products with digital elements — horizontal security requirements across the product lifecycle.
NIS2 Directive — (EU) 2022/2555	Medium and large entities in essential and important sectors — risk-management and incident-reporting duties, transposed nationally.
DORA — Reg (EU) 2022/2554	Financial entities and their critical ICT third-party providers — digital operational resilience for the financial sector.
Cybersecurity Act — Reg (EU) 2019/881	Providers seeking EU cybersecurity certification of ICT products, services and processes; sets ENISA’s mandate.
Cyber Solidarity Act — Reg (EU) 2025/38	Managed security service providers and critical-sector entities engaging with the EU cyber alert and reserve mechanisms.
eIDAS / eIDAS 2.0 — Reg (EU) 910/2014, am. 2024/1183	Trust-service providers and those relying on electronic identification, signatures and the forthcoming EU Digital Identity Wallet.
ISO/IEC 27001	Any organisation certifying an information-security management system — the baseline many customers and regulators expect.
ETSI EN 303 645	Makers of consumer IoT devices — the baseline security standard underpinning several product-security regimes.
ISO/IEC 29147 & 30111	Product teams running coordinated vulnerability disclosure and handling — referenced by the CRA and PSTI-type regimes.
Common Criteria — ISO/IEC 15408	Vendors seeking assurance-level security evaluation of IT products, often for public-sector or high-assurance buyers.

5. Product safety, conformity and liability

Framework	Who / what it applies to
Revised Product Liability Directive — (EU) 2024/2853	Manufacturers, importers and other operators of products — including software and AI — facing strict, no-fault civil liability for defective products.
General Product Safety Reg — (EU) 2023/988	Economic operators placing consumer products on the market — the safety net where no sector-specific rules apply.
Machinery Regulation — (EU) 2023/1230	Manufacturers of machinery and related products, including those with AI-driven safety functions.
Radio Equipment Directive — 2014/53/EU	Makers of radio and wireless-connected equipment — includes cybersecurity-relevant delegated requirements.
Low Voltage Directive — 2014/35/EU	Makers of electrical equipment within defined voltage ranges.
EMC Directive — 2014/30/EU	Makers of equipment that can cause or be affected by electromagnetic disturbance.
RoHS Directive — 2011/65/EU	Makers of electrical and electronic equipment — restricts hazardous substances.
Ecodesign for Sustainable Products — Reg (EU) 2024/1781	Makers of a widening range of products — sets sustainability, repairability and digital-product-passport requirements.
Medical Devices Reg — (EU) 2017/745	Makers of medical devices, including software that qualifies as a medical device.
In Vitro Diagnostic Reg — (EU) 2017/746	Makers of in-vitro diagnostic devices, including diagnostic software.
CE marking framework — Reg (EU) 765/2008 & Dec 768/2008	Manufacturers affixing CE marking — the horizontal accreditation and conformity-assessment machinery behind product directives.

6. Platforms, digital services and markets

Framework	Who / what it applies to
Digital Services Act — Reg (EU) 2022/2065	Intermediary services, hosting providers and online platforms — duties scale with size, heaviest for very large platforms and search engines.
Digital Markets Act — Reg (EU) 2022/1925	Designated “gatekeeper” platforms providing core platform services at scale.
Platform-to-Business Reg — (EU) 2019/1150	Online intermediation services and search engines, in their dealings with business users.
Terrorist Content Online — Reg (EU) 2021/784	Hosting service providers — one-hour removal duties for terrorist content.
Political Advertising Reg — (EU) 2024/900	Providers of political advertising services — transparency and targeting-restriction duties.
e-Commerce Directive — 2000/31/EC	Information-society service providers — foundational liability and information rules, now overlaid by the DSA.

7. Consumer protection and digital contracts

Framework	Who / what it applies to
Consumer Rights Directive — 2011/83/EU	Traders selling to consumers — pre-contract information and withdrawal rights, including for digital content and services.

Digital Content Directive — (EU) 2019/770	Traders supplying digital content or digital services to consumers — conformity and remedy rules.
Sale of Goods Directive — (EU) 2019/771	Traders selling goods, including goods with digital elements — including update obligations.
Unfair Commercial Practices — 2005/29/EC	Traders — bars misleading and aggressive practices, including many dark patterns.
Unfair Contract Terms — 93/13/EEC	Businesses using standard terms with consumers — unfair terms are not binding.
Omnibus Directive — (EU) 2019/2161	Traders — modernises consumer rules, price-transparency and penalties for online sales.
Geo-blocking Regulation — (EU) 2018/302	Traders selling across the EU — bars unjustified geo-blocking of customers by location.
PSD2 — Directive (EU) 2015/2366	Payment service providers and those offering payment-enabled digital services — strong customer authentication and access rules.

8. Accessibility

Framework	Who / what it applies to
European Accessibility Act — Dir (EU) 2019/882	Makers and sellers of specified products and services — e-commerce, banking, e-books, ticketing and more — must meet accessibility requirements.
Web Accessibility Directive — (EU) 2016/2102	Public-sector bodies — websites and mobile apps must meet accessibility standards.
EN 301 549	The harmonised standard used to demonstrate digital accessibility under both regimes above.

9. Intellectual property in digital products

Framework	Who / what it applies to
Copyright in the DSM — Dir (EU) 2019/790	Online content-sharing platforms, and anyone using text-and-data mining or protected content — includes the TDM exceptions relevant to AI training.
Database Directive — 96/9/EC	Makers and users of databases — protects substantial investment in database contents.
Trade Secrets Directive — (EU) 2016/943	Any business protecting confidential know-how — relevant to model weights, source code and datasets.
Software Directive — 2009/24/EC	Developers and users of computer programs — the specific copyright regime for software.

10. Governance, quality and assurance standards

Framework	Who / what it applies to
ISO 9001	Organisations certifying a general quality-management system — often the base an AI or product QMS builds on.
ISO/IEC 25010	Teams specifying and evaluating software product quality characteristics.
ISO/IEC 27017 / 27018	Cloud service providers and customers addressing cloud security and protection of personal data in the cloud.
ISO/IEC 27005	Teams needing a method for information-security risk management.
ISO 31000	Organisations wanting a general enterprise risk-management framework.
SOC 2 (AICPA)	Service organisations evidencing security, availability and confidentiality controls — US-origin but widely required by EU buyers.
ISAE 3402 / SOC 1	Service organisations reporting on controls relevant to customers' financial reporting.
EU Cloud Code of Conduct / CISPE	Cloud providers evidencing GDPR-aligned data protection through an approved code of conduct.
OWASP ASVS / Top 10	Development teams adopting recognised application-security best practice — not law, but a common assurance baseline.

11. Adjacent and sector-specific instruments worth knowing

Framework	Who / what it applies to

Interoperable Europe Act — Reg (EU) 2024/903	Public bodies and their suppliers — interoperability assessments for public-sector digital systems.
Chips Act — Reg (EU) 2023/1781	Semiconductor design and manufacturing actors — relevant to hardware-adjacent digital products.
Batteries Regulation — Reg (EU) 2023/1542	Makers of products containing batteries — includes a digital battery passport.
WEEE Directive — 2012/19/EU	Makers of electrical and electronic equipment — end-of-life take-back and recycling duties.
Whistleblowing Directive — (EU) 2019/1937	Organisations above size thresholds — must run internal reporting channels, often software-mediated.

Where to go next

(3) If several of these lines matched your product, that is normal — a modern digital product commonly sits inside a dozen or more of these instruments at once, and the hard part is not any single one but the way they overlap, borrow each other's standards, and stack liability. European Compliance Suite builds practical, ready-to-complete evidence templates for a growing set of these regimes — among them the AI Act, the Cyber Resilience Act, DORA, the Data Act, the revised Product Liability Directive, Swiss and UK digital law, and authorised-representative arrangements — each written to the primary text and designed to turn a regime you have identified here into documentation you can actually hold. If this map has shown you an exposure you had not mapped before, that is exactly what it was for.