Module	**Privacy and Data Protection**
Jurisdiction	**European Union**
Legal Expert	**Martin Polaine** Barrister (England & Wales), Brooke Chambers Barristers – BrookeChambers linkedin.com/in/martin-polaine-fciarb-faiadr-961363132

Module Application

Does an organisation implement measures to ensure lawful, secure, and accountable data processing, including data protection by design, DPIAs where required, and appoint a Data Protection Officer (DPO) when mandated?

Does the organisation maintain an up-to-date personal data register detailing categories of data collected, processing purposes, and data flows?

Does the organisation have a comprehensive privacy programme in place covering governance, risk management and accountability?

Does the organisation provide clear purposes for processing of personal data to data subjects and obtain valid, documented consent where required, supported by a consent management system, especially in sensitive areas such as healthcare?

Does the organisation have a structured process to respond to data subject requests (access, rectification, erasure, restriction, data portability, objection)?

Does the organisation implement robust security mechanisms to protect personal data from unauthorised access, loss, or breach, and are these controls regularly tested and updated?

Does the organisation lawfully manage cross-border data transfers (e.g., via SCCs, BCRs, or adequacy decisions), and conduct transfer impact assessments where appropriate?

Does the organisation embed privacy by design and by default into systems and processes, and regularly review and improve its data protection practices?

Does the organisation actively cooperate with supervisory authorities, comply with consistency mechanisms, and maintain documented procedures for representation, judicial remedies, and compensation claims?

Module Scope

EU Privacy and Data Protection is a regulatory framework that governs how organisations collect, process, and safeguard personal data within and beyond the European Union (EU). Anchored in the EU Charter of Fundamental Rights, it recognises data protection as a fundamental right and sets out clear rules to ensure that individuals' privacy is protected, data is processed lawfully, and organisations remain accountable for their practices. The framework aims to enforce transparency, control, and trust while enabling secure data flows across the EU.

The EU data protection regime is primarily governed by:

- The General Data Protection Regulation (GDPR) 2016
- The Law Enforcement Directive (LED) 2016
- The Data Protection Regulation for EU institutions (EUDPR) 2018

These instruments are further complemented by domain-specific laws, including the Digital Services Act (2022), Artificial Intelligence Act (2024), NIS 2 Directive (2022), Cybersecurity Act (2019), and the European Health Data Space Regulation (2025).

Together, they establish a harmonised data protection standard that applies across sectors and jurisdictions.

Applicability of the EU Privacy and Data Protection framework

The EU data protection framework applies to a wide range of organisations, including but not limited to:

- Organisations established in the EU: All entities located in the EU must comply with EU data protection laws when processing personal data, regardless of whether the processing occurs within or outside the EU.
- Non-EU organisations targeting the EU: Entities outside the EU that offer goods or services to individuals in the EU or monitor their behaviour within the EU are also subject to EU data protection obligations.
- Healthcare and high-risk sectors: Entities processing sensitive data, including health data or data involved in AI systems, must implement heightened safeguards due to the elevated risks involved.

Key requirements of the EU Privacy and Data Protection framework

- Data protection and processing framework: Organisations must base data processing on a valid legal basis (e.g. consent, contractual necessity, legal obligation) and comply with core data protection principles such as lawfulness, purpose limitation, minimisation, accuracy, and accountability.
- Accountability and role identification: Entities must clearly define their role as controllers, processors, or both, and implement technical and organisational safeguards, maintain records, and appoint representatives where required.
- Data subject rights: Organisations must enable individuals to exercise rights such as access, rectification, erasure, portability, and objection. Procedures must support transparency, timely response, and legal compliance.
- Risk assessments and DPIAs: Where data processing is likely to result in high risks, organisations must conduct Data Protection Impact Assessments (DPIAs), mitigate risks proactively, and consult supervisory authorities if needed.
- Appointment of a Data Protection Officer (DPO): In certain cases, a qualified and independent DPO must be designated to oversee compliance, advise on obligations, and act as a point of contact for authorities and individuals.
- Data breach notification and incident response: Organisations must detect, assess, and report personal data breaches within 72 hours to supervisory authorities and notify affected individuals when necessary. Breach records must be maintained.

- Cross-border data transfers: Transfers of personal data outside the EU must comply with EU requirements, such as using Adequacy Decisions, Standard Contractual Clauses (SCCs), or Binding Corporate Rules (BCRs), supported by Transfer Impact Assessments where applicable.
- Vendor and third-party management: Organisations must assess and monitor processors handling personal data to ensure GDPR compliance, secure contracts, audit rights, sub-processor controls, and appropriate security measures throughout the supply chain.
- Workplace privacy and employee data: Employers must ensure transparency and lawfulness when processing employee data, implement proportionate safeguards, and address special rules for monitoring and sensitive data.
- Employee training and awareness: Organisations must provide data protection training tailored to roles and risks, ensuring all personnel understand legal obligations, proper handling procedures, and the role of the DPO.
- Health data protection: Entities processing health data must meet strict requirements for consent, security, and lawful use, with robust risk-based measures to ensure confidentiality, integrity, and resilience.

Our expert's profile

MARTIN POLAINE
Barrister

PRACTICE AREAS

International Arbitration, Regulatory and Compliance (including corporate investigations, ESG, anti-corruption, AML/financial regulatory and sports governance), Public International Law, International Trade, Corporate and Institutional Governance

BROOKE CHAMBERS

MARTIN POLAINE is a barrister (England & Wales) of more than 35 years' experience and an arbitrator. He is a Fellow of both the Chartered Institute of Arbitrators (FCIArb) and a Fellow of the Asian Institute of Alternative Dispute Resolution (FAIADR).

Martin has advised states, corporates and individuals across Africa, Asia and Europe on dispute resolution and public international law. He has extensive experience in both civil law and common law states and his practice includes international arbitration (both commercial and state-investor), regulatory and compliance (including corporate investigations, ESG, anti-corruption, AML/financial regulatory and sports governance), public international law, international trade and most aspects of corporate and institutional governance.

Having a keen interest in professional regulation, Martin has advised law societies and other professional bodies on a range of issues, including the use of quality assurance standards (Lexcel, ISO standards and others), the drafting of codes of conduct and financial regulatory compliance.

He is a published author of legal texts (with Oxford University Press and others), a Teaching Fellow at the College of Law (Sydney), where he tutors LLM students, and Co-Chair of the Inter-Pacific Bar Association's Legal Training & Development Committee.

About LexisNexis Regulatory Compliance®

LexisNexis Regulatory Compliance® helps you forge a clear path to compliance.

With LexisNexis® content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.
