GPDP

Global Privacy & Data Protection Practitioner

6-Day Training Programme | 48 Hours | 6 Domains

A comprehensive practitioner programme drawing from IAPP CIPP/E, CIPM, CIPT, ISO 27701, GDPR, CCPA, PDPA, LGPD and all major global privacy frameworks — designed for professionals, managers and entire organisational teams.

Suitable for all organisations worldwide

1. Course Overview

The Global Privacy & Data Protection Practitioner (GPDP) programme is a comprehensive 6-day training course that equips both management and operational teams with the knowledge, skills and practical tools to build and sustain a world-class privacy programme.

Unlike single-jurisdiction certifications, GPDP takes a deliberately global approach — covering all major privacy laws, governance standards and technical frameworks in an integrated, practical curriculum. Participants leave with the ability to apply privacy principles across any regulatory environment, in any sector, and in any part of the world.

Course Identity

Field	Details
Course Name	Global Privacy & Data Protection Practitioner (GPDP)
Duration	6 days — 8 hours per day — 48 hours total
Format	Instructor-led with scenarios, group discussions and practical exercises
Domains	6 core domains covering law, governance, technology, rights, culture and AI
Suitable For	All organisations — corporate, public sector, NGOs — worldwide
Languages	Adaptable — core materials in English with localisation support

2. Course Objectives

On successful completion of the GPDP programme, participants will be able to:

- Understand the global privacy law landscape and identify which regulations apply to their organisation
- Build and manage an effective privacy programme aligned to international best practice
- Conduct Data Protection Impact Assessments (DPIAs) and manage data inventories
- Implement Privacy by Design principles in products, systems and processes
- Manage data subject rights requests efficiently and within required timelines
- Respond to personal data breaches with confidence and legal compliance
- Develop privacy training programmes that build a culture of compliance
- Advise senior leadership on privacy risk, regulatory developments and accountability
- Navigate international data transfers and third-party vendor privacy obligations
- Understand AI privacy risks and how emerging regulations apply to automated systems
- Prepare for leading privacy certifications including IAPP CIPP, CIPM and CIPT

3. Target Audience

GPDP is designed as a complete organisational training solution, relevant to both leadership and operational roles. The content is structured so that every participant — regardless of their function — gains practical, applicable knowledge throughout all six days.

Leadership & Management	Team & Practitioner Roles
DPOs and Privacy Officers	Developers and Engineers
Legal and Compliance Managers	Marketing and CRM Teams
HR and People Managers	Customer Service Staff
IT and Security Managers	Finance and Procurement
Risk and Audit Leads	Data Analysts and Scientists
C-Suite and Senior Leadership	Product and Project Managers

4. Referenced Frameworks & Certifications

The GPDP curriculum draws on and integrates topics from the following privacy certification bodies, regulations and standards:

IAPP CIPP/E	IAPP CIPP/US	IAPP CIPP/A	IAPP CIPM	IAPP CIPT
EU GDPR	UK GDPR	CCPA / CPRA	LGPD (Brazil)	PIPEDA (Canada)
PDPA (Singapore)	PIPL (China)	POPIA (S. Africa)	ISO 27701	ISO 27001
NIST Privacy Fwk	FIPPs	HIPAA	ePrivacy Directive	EU AI Act

By synthesising the best elements from each of these sources into a single coherent programme, GPDP ensures participants develop transferable knowledge that is not tied to any single certification or jurisdiction.

5. 6-Day Programme At a Glance

Domain Overview

Domain	Title
Domain 1	Law, Regulation & Jurisdictions
Domain 2	Governance & Programme Management
Domain 3	Technology & Privacy by Design
Domain 4	Rights, Ethics & Transparency
Domain 5	Incidents, Audit & Culture
Domain 6	AI, Emerging Tech & Future Compliance

Daily Summary

Day	Module Title	Domain
Day 1	**Privacy Foundations & Global Legal Landscape**	Domain 1 — Law, Regulation & Jurisdictions
Day 2	**Data Governance, DPIA & Privacy Programme Management**	Domain 2 — Governance & Programme Management
Day 3	**Privacy Engineering, Technology & Security Controls**	Domain 3 — Technology & Privacy by Design
Day 4	**Individual Rights, Ethics & Transparency**	Domain 4 — Rights, Ethics & Transparency
Day 5	**Incident Management, Culture & Continuous Compliance**	Domain 5 — Incidents, Audit & Culture
Day 6	**AI, Emerging Technologies & Future of Privacy**	Domain 6 — AI, Emerging Tech & Future Compliance

Day 1 — Privacy Foundations & Global Legal Landscape

Domain 1: Law, Regulation & Jurisdictions | 8 Hours

Day 1 establishes the foundational knowledge every privacy professional and team member needs. Participants explore the philosophy behind privacy law, understand why privacy protection matters to organisations, and gain a thorough grounding in the global regulatory landscape — from the EU's GDPR to Asia-Pacific frameworks and the Americas.

Session	Topics Covered
Session 1 Privacy Foundations & Core Principles	• Privacy as a fundamental human right • Fair Information Practice Principles (FIPPs) • Privacy vs. security vs. confidentiality — understanding the distinctions • A brief history of privacy law and why it matters today • Why privacy protection is a business priority, not just a legal obligation
Session 2 Global Legal Frameworks — EU & UK	• GDPR deep dive: key definitions, lawful bases and territorial scope • UK GDPR post-Brexit: what has changed and what remains the same • Data controller vs. processor obligations and responsibilities • Role of Data Protection Authorities (DPAs) and their enforcement powers • Notable enforcement cases and lessons for practitioners
Session 3 Global Legal Frameworks — Americas & APAC	• CCPA/CPRA (California), LGPD (Brazil), PIPEDA (Canada) • PDPA (Singapore and Thailand), PIPL (China), POPIA (South Africa) • Cross-border data transfer mechanisms and key obligations • Comparing the key requirements across major jurisdictions
Session 4 Sector-Specific Rules & Special Categories of Data	• Healthcare data: HIPAA highlights and global equivalents • Financial sector: GLBA, PSD2 and banking data rules • Children's data: COPPA and GDPR Article 8 requirements • Biometric, health and genetic data — special category rules • Sensitive data categories compared across jurisdictions
Session 5 Practical Application: Jurisdiction Mapping	• How to map an organisation's operations to applicable laws • Building a jurisdiction inventory — approach and template • Identifying which regulations apply to your organisation • Group discussion: privacy responsibilities across different roles • Key takeaways and recap of Day 1

Day 2 — Data Governance, DPIA & Privacy Programme Management

Domain 2: Governance, Accountability & Programme Management | 8 Hours

Day 2 moves from theory to practice, equipping participants with the operational tools to build and run a privacy programme. The day covers governance structures, DPO responsibilities, data mapping, DPIAs and managing international data transfers.

Session	Topics Covered
Session 1 Building a Privacy Programme	• Privacy governance structures and how to set them up • DPO appointment, role, independence and authority • Assigning privacy responsibilities across business units • Privacy steering committees and escalation processes • Accountability frameworks and ISO 27701 overview
Session 2 Records of Processing & Data Mapping	• Article 30 Records of Processing Activities (ROPA) requirements • Data inventory and data mapping techniques • Creating and reading data flow diagrams • Vendor and third-party mapping • Maintaining living records as organisations evolve
Session 3 Data Protection Impact Assessments (DPIA)	• When DPIAs are legally required • Step-by-step DPIA methodology • Risk identification, scoring and prioritisation • Consulting the supervisory authority when required • Integrating DPIAs into project and product lifecycles
Session 4 Contracts, Vendors & International Transfers	• Data Processing Agreements (DPAs): essential clauses • Standard Contractual Clauses (SCCs) — updated sets • Binding Corporate Rules (BCRs) and adequacy decisions • Transfer Impact Assessments: when and how to conduct them • Vendor due diligence and ongoing monitoring
Session 5 Applied Learning: Conducting a DPIA	• Guided DPIA exercise on a realistic scenario • Identifying risks and proposing mitigations • Presenting DPIA findings clearly to stakeholders • Embedding DPIAs into project governance processes • Day 2 recap and key learning points

Day 3 — Privacy Engineering, Technology & Security Controls

Domain 3: Technology, Systems & Privacy by Design | 8 Hours

Day 3 bridges the gap between legal compliance and technical implementation. Participants learn how to embed privacy into product development and systems design, manage consent infrastructure, apply security controls, and address privacy risks in cloud services.

Session	Topics Covered
Session 1 Privacy by Design & by Default	• Seven foundational principles of Privacy by Design • Data minimisation in system and product design • Purpose limitation in architecture decisions • Overview of Privacy-Enhancing Technologies (PETs) • Integrating privacy into Agile and DevOps workflows
Session 2 Consent Management & Tracking Technologies	• Valid consent: freely given, specific, informed and unambiguous • Consent Management Platforms (CMPs) and their architecture • Cookie compliance: ePrivacy Directive requirements explained • Dark patterns in consent UX — what to avoid • Managing consent lifecycle, withdrawal and records
Session 3 Data Security & Encryption Fundamentals	• CIA triad applied to personal data protection • Encryption at rest and in transit: practical overview • Pseudonymisation vs. anonymisation — legal significance • Access controls and the principle of least privilege • Relevant standards: ISO 27001 and NIST Cybersecurity Framework
Session 4 Cloud, SaaS & Third-Party Technology Risk	• Cloud computing privacy risk — IaaS, PaaS, SaaS distinctions • Assessing privacy risks in SaaS procurement • Shared responsibility model and where privacy obligations sit • Managing third-party data processors in cloud environments • Practical checklist for cloud vendor privacy evaluation
Session 5 Applied Learning: Privacy by Design Review	• Review a sample application or system for privacy risks • Identify gaps and propose Privacy by Design controls • How to present technical privacy findings to non-technical stakeholders • Embedding privacy review gates in project governance • Day 3 recap and consolidation

Day 4 — Individual Rights, Ethics & Transparency

Domain 4: Data Subject Rights, Ethics & Accountability | 8 Hours

Day 4 focuses on the individual — both as a data subject whose rights must be respected, and as an employee whose workplace privacy deserves protection. Participants gain practical skills in handling rights requests, drafting transparent privacy notices and applying ethical thinking to data decisions.

Session	Topics Covered
Session 1 Data Subject Rights — Full Lifecycle	• Right of access (Subject Access Request — SAR) • Right to rectification, erasure and restriction of processing • Right to data portability and right to object • Rights related to automated decision-making • Response timelines, identity verification and valid exemptions
Session 2 Privacy Notices & Transparency Obligations	• Layered privacy notice approach • GDPR Articles 13 and 14 requirements in full • Writing clear, plain-language privacy notices • Staff privacy notices and employment context • Global privacy notice comparison across jurisdictions
Session 3 Employee & Workplace Privacy	• Monitoring employees: legal limits and proportionality • BYOD policies, remote work and hybrid arrangements • Recruitment, HR data handling and background checks • Whistleblowing, confidentiality and consent in employment • Remote and hybrid work privacy risks
Session 4 Privacy Ethics, Fairness & Responsible Data Use	• Ethical frameworks for data-related decisions • Algorithmic fairness and bias in automated systems • Privacy as a business value, not merely a compliance exercise • Ethical considerations for data sharing and secondary use • Privacy at the intersection of human rights
Session 5 Applied Learning: Subject Access Request Simulation	• End-to-end SAR exercise: receive, verify, search, redact, respond • Working through exemptions and complex real-world scenarios • Building a repeatable SAR process workflow • Quality-checking a response before sending • Day 4 recap and key lessons

Day 5 — Incident Management, Culture & Continuous Compliance

Domain 5: Breach Response, Audit, Culture & Regulatory Readiness | 8 Hours

Day 5 addresses what happens when things go wrong and how to build the organisational culture and continuous improvement mechanisms to prevent recurrence. Participants develop incident response skills, learn how to conduct a privacy audit and explore the regulatory landscape ahead.

Session	Topics Covered
Session 1 Data Breach Management & Incident Response	• Defining a personal data breach under GDPR and globally • The 72-hour notification rule: triggers, process and documentation • Breach severity assessment and risk-to-individuals scoring • Notifying data subjects: when and how • Maintaining a breach register and post-incident review
Session 2 Privacy Audits, Reviews & Continuous Monitoring	• Privacy audit methodology: planning, fieldwork and reporting • Internal vs. external privacy audits — when to use each • Privacy programme maturity models • Key privacy KPIs and performance metrics • Documentation, evidence management and regulatory inspection readiness
Session 3 Building a Privacy-Aware Culture	• Principles of effective privacy awareness training • Role-based training content for different functions • Privacy champions networks and ambassador programmes • Building the business case for senior leadership buy-in • Measuring culture change and awareness effectiveness
Session 4 Enforcement, Fines & Regulatory Trends	• GDPR enforcement actions: key cases and lessons learned • ICO, CNIL and other DPA enforcement patterns • How fines are calculated and contextualised • Regulatory trends from 2024 through 2026 • Preparing your organisation for the next wave of regulation
Session 5 Programme Review & Certification Pathways	• Full programme gap analysis exercise • Mapping your organisation against a maturity model • Individual action planning: 30/60/90-day next steps • IAPP certification pathways: CIPP, CIPM and CIPT explained • Course Q&A, resources and close of Day 5

Day 6 — AI, Emerging Technologies & The Future of Privacy

Domain 6: AI, Emerging Tech & Future Compliance | 8 Hours

Day 6 is a forward-looking module that equips participants with the knowledge and practical skills to navigate privacy in the age of artificial intelligence, big data and rapidly evolving technology. It covers the EU AI Act, automated decision-making, biometrics and IoT — concluding with a capstone privacy programme assessment.

Session	Topics Covered
Session 1 AI Fundamentals & Privacy Risks	• How AI and machine learning systems process personal data • Key privacy risks in AI model training, testing and deployment • Bias, fairness and transparency in automated systems • GDPR Article 22: automated decision-making and profiling • The principle of human oversight in AI systems
Session 2 EU AI Act & Global AI Governance	• EU AI Act: structure, risk tiers and compliance obligations • High-risk AI systems and the requirements that apply • AI transparency, explainability and documentation requirements • International AI governance frameworks: NIST AI RMF, OECD AI Principles • What AI regulation means for your organisation in practice
Session 3 Biometrics, IoT & Connected Technologies	• Biometric data: definition, risks and governance requirements • Facial recognition: legal landscape and proportionality tests • IoT and connected device privacy challenges • Smart buildings, wearables and employee monitoring technologies • Applying Privacy by Design to IoT systems
Session 4 Big Data, Analytics & Responsible Innovation	• Privacy risks inherent in large-scale data analytics • Anonymisation at scale: challenges and limitations • Synthetic data and privacy-preserving analytics techniques • Ethical data science: balancing innovation with individual rights • Building responsible data practices into analytics workflows
Session 5 Capstone: Privacy Programme Assessment	• Comprehensive privacy programme gap analysis exercise • Applying all six domains to a realistic organisational scenario • Presenting findings and recommendations as a practitioner • Individual 30/60/90-day privacy improvement action plan • Final Q&A, certification pathways review and course close

Onward Certification Pathways

GPDP is designed to accelerate progress towards leading privacy certifications. The table below maps recommended next steps for different roles:

Certification	Body	Recommended For
CIPP/E	IAPP	Legal, compliance and DPO roles — strong GDPR focus
CIPP/US	IAPP	Organisations with significant US operations or customers
CIPM	IAPP	Privacy managers, DPOs and programme leads
CIPT	IAPP	Developers, IT professionals and technology teams
ISO 27701 Lead Implementer	Various	Governance and audit roles, especially in regulated sectors