TRANCHULAS

PROFESSIONAL PRACTITIONER COURSE

European Data Protection & GDPR

Applied European privacy practice

Turn legal sources, facts and risk into defensible operational decisions.

3	12	9	40
FOCUSED DAYS	APPLIED MODULES	LANDMARK JUDGMENTS	ASSESSMENT QUESTIONS

For people who make privacy decisions in the real world advising product teams, negotiating supplier contracts, responding to rights requests, reviewing incidents and challenging assumptions in project meetings.

Explore dates and enrolment at tranchulas.com

CREST CYBER

Most privacy advice fails not because the law was misread, but because the facts were never established.

This intensive three-day programme is built for the moment a decision has to be made and defended when a product team wants an answer today, a supplier will not disclose where its engineers sit, or a regulator asks why an organisation considered something acceptable.

Participants work through twelve applied modules, five recurring case organisations and concise fact patterns drawn from real advisory situations. Each module moves between legal rules, operational judgment and a scenario in which the material facts are deliberately incomplete.

Three categories, never collapsed

Every proposition is marked as legal requirement, regulatory interpretation or good practice the distinction that separates a defensible position from an opinion.

Facts before conclusions

Scenarios deliberately leave material facts open. The stronger answer names what must be established, documented or escalated first.

Five organisations, twelve modules

The same five case organisations recur throughout, so decisions compound rather than resetting with each topic.

Written to be maintained

Time-sensitive propositions are tracked in a Legal Update Register with recheck triggers and authoritative sources against each entry.

Who it is for

Privacy and data protection officers

Practitioners who must defend a decision, not just cite an article.

Legal and compliance counsel

Advisers translating GDPR into positions a business can actually operate.

Security and risk leaders

Owners of Article 32, breach response and the NIS2 boundary.

Product, engineering and procurement

Teams whose design and vendor choices set the compliance position.

CREST CYBER

Tranchulas is a CREST Cyber Training Provider, validating the excellence and credibility of our training offerings.

What you will be able to do

By the end of the course, participants will be able to apply the following capabilities in operational privacy work.

01 Identify the governing legal regime for a European privacy question and select authoritative sources, distinguishing legal requirement from regulatory interpretation and good practice.

02 Apply GDPR material and territorial scope to international business scenarios, including establishment, targeting and behavioural monitoring.

03 Distinguish personal, pseudonymised and anonymous data, and evaluate re-identification risk against realistically available means.

04 Allocate controller, joint-controller, processor and sub-processor roles by analysing actual processing activities rather than contractual labels.

05 Select and document a lawful basis under Article 6, including structured legitimate-interests assessments and the two-stage Article 9 analysis.

06 Design transparent information and operate individual rights requests from receipt to documented response within statutory deadlines.

07 Map international transfers, including remote access, and select Chapter V mechanisms with effective supplementary measures.

08 Assess workplace monitoring, direct marketing and online tracking proposals for necessity, proportionality and national-law compliance.

09 Analyse cloud and AI deployments across roles, purposes, automated decision-making and the interface with the EU AI Act.

10 Classify personal-data breaches, apply the Article 33 and Article 34 thresholds, and distinguish GDPR duties from NIS2 reporting.

11 Build proportionate accountability evidence, including records of processing, retention governance and data protection impact assessments.

12 Prepare an evidence-based response to a supervisory authority inquiry and anticipate corrective, civil and reputational exposure.

How the three days are structured

DAY 1

Legal foundations, scope, roles and lawful processing

Modules 1–4

DAY 2

Rights, international transfers, workforce and marketing

Modules 5–8

DAY 3

Technology, security, governance and enforcement

Modules 9–12 and final assessment

Legal Foundations, Scope, Roles and Lawful Processing

Establish which regime governs, classify the data and the roles, then choose and evidence a lawful basis.

Module 1

European Privacy Law — Foundations and Architecture

- The Council of Europe, the ECHR and the European Court of Human Rights
- The EU Charter, Articles 7 and 8, and the role of the GDPR
- The Law Enforcement Directive, the EUDPR and the ePrivacy Directive
- National supervisory authorities, the EDPB, the EDPS and the Commission
- The CJEU and the ECtHR: two courts, two legal systems
- Building a working source hierarchy for compliance questions

EXERCISE Select the governing source sequence for a cross-border analytics decision

Module 2

Scope, Personal Data and Data Classification

- Material and territorial scope under Articles 2 and 3
- Establishment, market targeting and behavioural monitoring
- Direct and indirect identification; online and device identifiers
- Pseudonymisation versus anonymisation and re-identification risk
- Special-category data and the two-stage Article 6 and Article 9 analysis
- Criminal-offence data under Article 10 and national-law conditions

CASE Breyer (C-582/14) and realistically available means of identification

EXERCISE Determine whether a coded customer dataset can be released as anonymous

Module 3

Roles, Responsibility and Supplier Ecosystems

- Activity-based determination of controller and processor roles
- Joint controllers and transparent allocation under Article 26
- Sub-processors, recipients and third parties in a supply chain
- Article 28 processor terms and operational vendor governance
- EU and UK representatives and the Data Protection Officer function

CASE Fashion ID (C-40/17) and third-party plugins and pixels

EXERCISE Allocate roles across a co-branded campaign and a hosted SaaS platform

Module 4

Principles and Lawful Processing

- The Article 5 principles applied as a design test
- The six Article 6 lawful bases and the test each one imposes
- Contract necessity and the limits of terms and conditions
- Consent: validity, power imbalance, granularity and withdrawal
- Legitimate interests: purpose, necessity and the balancing exercise
- Purpose limitation and compatible further processing under Article 6(4)

CASE Meta Platforms (C-252/21) and objective contract necessity

EXERCISE Build a defensible lawful-basis record for a fraud-detection model

Rights, International Transfers, Workforce and Marketing

Make rights operational, move data across borders defensibly, and hold the line in the workplace and the marketing stack.

Module 5

Transparency and Individual Rights

- Articles 12 to 14: layered, timely and intelligible information
- Access, rectification, erasure and restriction in operational practice
- Portability: conditions, scope and the limits of derived data
- The right to object and proportionate direct-marketing suppression
- Profiling distinguished from Article 22 automated decisions

CASE SCHUFA (C-634/21) and scoring within a decision chain

EXERCISE Operate a rights request from receipt to documented response

Module 6

International Transfers and Cross-Border Processing

- Identifying a Chapter V transfer, including remote and administrator access
- Adequacy decisions and the EU–US Data Privacy Framework
- The EU–UK position and mapping transfers in both directions
- Standard Contractual Clauses and selecting the correct module
- Binding Corporate Rules, codes of conduct and certification
- Transfer impact assessment and effective supplementary measures
- Article 49 derogations and Article 48 third-country authority demands

CASE Schrems II (C-311/18) and essential equivalence

EXERCISE Build a transfer file for a third-country support and hosting model

Module 7

Workforce Data and Surveillance

- Recruitment, the employment lifecycle and retention discipline
- Article 88, national labour law and collective agreements
- Consent and the employment power imbalance
- Monitoring, BYOD, CCTV, location tracking and biometric access control
- Whistleblowing systems, investigations and fairness to named persons

CASE Bărbulescu v Romania (ECtHR, Grand Chamber)

EXERCISE Test a workplace monitoring proposal for necessity and proportionality

Module 8

Marketing, Cookies and Digital Services

- Direct marketing and the absolute right to object under Article 21
- The ePrivacy Directive and its national implementation
- Terminal-equipment rules, strictly necessary exceptions and consent
- Online identifiers, profiling, audience sharing and sensitive inferences
- Deceptive design patterns that undermine valid consent

CASE Planet49 (C-673/17) and pre-ticked consent

EXERCISE Audit a cookie banner and a purchased marketing list

Technology, Security, Governance and Enforcement

Take the analysis into cloud and AI deployments, incidents, governance evidence and the regulator's inbox.

Module 9

Cloud, AI and Emerging Technology

- Activity-based analysis of cloud services, sub-processing and support access
- GDPR across the AI lifecycle: sourcing, training, deployment and monitoring
- Prompts, outputs, telemetry and model-improvement as separate purposes
- Article 22 in AI deployments and meaningful human involvement
- GDPR and the EU AI Act as distinct regimes with distinct actors

EXERCISE Run a pre-procurement review of a generative-AI vendor

Module 10

Security and Incident Response

- Article 32 measures appropriate to risk rather than a fixed technology list
- Confidentiality, integrity, availability and resilience objectives
- Supplier security assurance and the shared responsibility boundary
- Personal-data breach classification and the Article 33 risk threshold
- Article 34 communication, effective mitigation and phased notification
- NIS2 and GDPR as separate reporting regimes

CASE Natsionalna agentsia za prihodite (C-340/21)

EXERCISE Take a ransomware incident to a documented notification decision

Module 11

Accountability by Design and Governance

- Article 5(2) and Article 24 accountability frameworks in proportion to risk
- Records of processing activities and purpose-led retention governance
- Data protection by design and by default under Article 25
- DPIA methodology, residual risk and Article 36 prior consultation
- DPO designation, independence and conflicts of interest

EXERCISE Rebuild a records-of-processing entry and screen a project for DPIA

Module 12

Supervision, Remedies and Enforcement

- Supervisory authority investigative and corrective powers
- The EDPB, the EDPS and the consistency mechanism
- Cross-border processing, main establishment and the one-stop shop
- Complaints, judicial remedies and Article 82 compensation
- Article 83 fining criteria and the range of corrective measures
- Responding to a regulator inquiry as a cross-functional team

CASE Österreichische Post (C-300/21) and non-material damage

EXERCISE Prepare a first response plan to a cross-border complaint

FINAL ASSESSMENT AND DEBRIEF

Forty-question applied assessment spanning all twelve modules · Best-answer, multiple-response and open-fact scenario formats · Structured debrief with defensible-answer rationale · Individual feedback and post-course remediation guidance

Built on judgments, not slogans

The course teaches nine landmark judgments as working tools, and runs every module against the same five organisations so that decisions compound.

Landmark judgments taught

Breyer C-582/14
When an identifier becomes personal data

Fashion ID C-40/17
Controllership for embedded third-party tags

Meta Platforms C-252/21
The limits of contract necessity

SCHUFA C-634/21
When a score becomes an Article 22 decision

Schrems II C-311/18
Transfer safeguards and essential equivalence

Planet49 C-673/17
Pre-ticked consent and terminal equipment

Bărbulescu v Romania ECtHR GC
Proportionality in workplace monitoring

Natsionalna agentsia za prihodite C-340/21
Article 32 judged against risk, not hindsight

Österreichische Post C-300/21
Infringement, damage and causation

Recurring case organisations

Asteron Retail Group
Loyalty programme, mobile app, advertising partners and analytics

Orion Health Systems
Health technology serving hospitals across several EEA states

Harbour Talent Partners
Recruitment and workforce analytics in the EEA and the UK

VertexCloud Services
SaaS collaboration and identity management

Nexa Finance Europe
Payments, fraud detection, onboarding and mobile banking

These organisations are fictional and are not based on any real organisation or supplier.

Applied throughout

Practical examples, decision points and scenario labs in every module, with the material facts deliberately left open.

Assessed at the end

A 40-question paper in best-answer, multiple-response and scenario formats, debriefed in blocks with defensible-answer rationale.

Maintained after delivery

Time-sensitive propositions are tracked in a Legal Update Register with recheck triggers and authoritative sources.

TRANCHULAS

Ready to strengthen your privacy practice?

Explore course dates, discuss team delivery or request enrolment information for the European Data Protection and GDPR Professional Practitioner Course.

WEB

tranchulas.com

EMAIL

info@tranchulas.com