Confidentiality, Data Protection & Legal Notice

A Comprehensive Multi-Jurisdictional Legal Framework Document

The Institute for Counselling & Psychotherapy Studies

ICPS College, Dublin, Ireland

DOCUMENT TYPE	Confidentiality, Data Protection & Legal Notice
INSTITUTION	ICPS College
PROVIDER NO.	PDCD1110 · CPD Standards Office
JURISDICTION	Ireland • United Kingdom • European Union • International

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

TABLE OF CONTENTS

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

— ECHR Article 8
— Convention 108 & 108+
— Budapest Convention
— UDHR Article 12
— OECD Privacy Guidelines
— APEC Framework
— ISO/IEC 27001 & 27701

PART VI Application to ICPS College — Obligations & Procedures

— Learner Data
— Staff Data
— Clinical Records
— Recorded Lectures & Communications
— Breach Procedures
— Data Subject Rights in Practice

PART VII Key Legal Quotations & Statutory Extracts

— Statutory Extracts
— Case Law Quotations
— Regulatory Guidance Quotations

PART VIII Legal References — 200 Citations

— 200 Numbered Legal References

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

PART I — FOUNDATIONAL PRINCIPLES OF DATA PROTECTION & PRIVACY

Data protection and privacy law rests upon a body of principles that has evolved over more than five decades, beginning with national legislative experiments in the 1970s and maturing into a sophisticated, internationally harmonised framework. This Part sets out the foundational principles that underpin all subsequent sections of this document.

1.1 The Right to Privacy as a Fundamental Right

Privacy is recognised as a fundamental human right across all major legal systems covered by this document. The right is grounded in personal autonomy, dignity and the freedom of individuals to control information about themselves. It enables participation in democratic society and is a precondition for the exercise of other rights, including freedom of expression and freedom of association.

> *"Everyone has the right to respect for his private and family life, his home and his correspondence."*
>
> European Convention on Human Rights (1950), Article 8(1)

> *"Everyone has the right to the protection of personal data concerning him or her."*
>
> Charter of Fundamental Rights of the European Union (2000), Article 8(1)

The ECHR right to privacy under Article 8 is qualified — interferences are permissible only where they are in accordance with law, pursue a legitimate aim, and are necessary in a democratic society. This proportionality test has been applied extensively by the European Court of Human Rights (ECtHR) and has profoundly shaped domestic data protection law throughout Europe.

1.2 The Seven Data Protection Principles

Article 5 of the General Data Protection Regulation (GDPR) (EU) 2016/679 codifies seven core data protection principles, to which all processing of personal data must conform. These principles are replicated in substance across Irish, UK and international data protection instruments:

- **Lawfulness, Fairness and Transparency** — Data must be processed lawfully, fairly and in a transparent manner in relation to the data subject (Art. 5(1)(a)).
- **Purpose Limitation** — Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Art. 5(1)(b)).
- **Data Minimisation** — Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Art. 5(1)(c)).
- **Accuracy** — Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay (Art. 5(1)(d)).
- **Storage Limitation** — Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (Art. 5(1)(e)).
- **Integrity and Confidentiality** — Data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (Art. 5(1)(f)).

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

- **Accountability** — The controller is responsible for, and must be able to demonstrate compliance with, the foregoing principles (Art. 5(2)).

> *"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability)."*
>
> GDPR (EU) 2016/679, Article 5(2)

1.3 Lawful Basis for Processing (Article 6 GDPR)

Processing of personal data is lawful only where at least one of the following six bases in Article 6(1) applies:

- Consent — the data subject has given clear consent to the processing of their personal data for one or more specific purposes (Art. 6(1)(a)).
- Contract — processing is necessary for the performance of a contract to which the data subject is party, or to take pre-contractual steps (Art. 6(1)(b)).
- Legal Obligation — processing is necessary for compliance with a legal obligation to which the controller is subject (Art. 6(1)(c)).
- Vital Interests — processing is necessary to protect the vital interests of the data subject or another natural person (Art. 6(1)(d)).
- Public Task — processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Art. 6(1)(e)).
- Legitimate Interests — processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights of the data subject (Art. 6(1)(f)).

1.4 Special Category Data (Article 9 GDPR)

Article 9 GDPR prohibits the processing of special categories of personal data unless a specific condition in Article 9(2) is satisfied. Special categories include data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data processed for uniquely identifying a natural person; health data; and data concerning a person's sex life or sexual orientation.

> *"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."*
>
> GDPR (EU) 2016/679, Article 9(1)

In the context of counselling and psychotherapy education — such as that delivered by ICPS College — mental health and health-related disclosures are special category data and attract the highest level of protection. Explicit consent under Article 9(2)(a) or a substantial public interest basis under Article 9(2)(g) is typically required.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

1.5 Data Subject Rights under GDPR

Chapter III of the GDPR (Articles 12–23) confers a comprehensive suite of rights upon data subjects. These rights must be exercised free of charge and responded to within one calendar month (extendable to three months for complex requests). The principal rights are:

- **Right of Access (Art. 15)** — the right to obtain confirmation of whether personal data is being processed, and if so, access to that data together with supplementary information.
- **Right to Rectification (Art. 16)** — the right to have inaccurate personal data corrected and incomplete data completed.
- **Right to Erasure / Right to be Forgotten (Art. 17)** — the right to have personal data deleted in certain specified circumstances.
- **Right to Restriction (Art. 18)** — the right to restrict the processing of personal data in certain circumstances.
- **Right to Data Portability (Art. 20)** — the right to receive personal data in a structured, commonly used machine-readable format and to transmit it to another controller.
- **Right to Object (Art. 21)** — the right to object to processing based on legitimate interests or in the public interest, including for direct marketing.
- **Rights related to automated decision-making (Art. 22)** — the right not to be subject to a decision based solely on automated processing which produces significant effects.

1.6 Privacy by Design and by Default (Article 25 GDPR)

Article 25 GDPR requires controllers to implement technical and organisational measures to give effect to data protection principles both at the time of designing the processing and at the time of the processing itself. Only personal data which is necessary for each specific purpose of the processing is to be processed by default.

> *"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."*
>
> GDPR (EU) 2016/679, Article 25(2)

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

PART II — IRISH LAW

Ireland has implemented a comprehensive domestic data protection and confidentiality framework consistent with EU law obligations. This Part surveys the principal legislative instruments applicable to the operations of ICPS College.

2.1 Data Protection Act 2018 (Ireland)

The Data Protection Act 2018 is the primary Irish statute giving domestic effect to the GDPR and repealing and replacing the Data Protection Acts 1988–2003. It designates the Data Protection Commission (DPC) as the national supervisory authority (s. 10), with functions including the investigation and adjudication of complaints (ss. 109–113), the conduct of inquiries (s. 110), and the imposition of administrative sanctions. The DPC may also bring court proceedings for infringements (s. 134).

> *"A controller or processor shall not process personal data except in accordance with the requirements of this Act and the GDPR."*
>
> Data Protection Act 2018 (Ireland), s. 99

Section 36 of the Act permits restrictions on data subject rights where necessary to safeguard important objectives of public interest, including prevention, investigation, detection and prosecution of criminal offences. Section 69 makes separate provision for academic, journalistic and artistic processing, applying a proportionality assessment. The Act also creates criminal offences for: unlawfully obtaining or disclosing personal data (s. 144); obstructing or hindering the DPC (s. 148); and failure to comply with an enforcement notice (s. 140).

2.2 Criminal Justice (Offences Relating to Information Systems) Act 2017

This Act transposes the EU Directive on Attacks Against Information Systems (2013/40/EU) into Irish law. It creates a range of computer-related criminal offences central to the protection of digital communications and data.

- **Section 2** — Unlawful access to an information system: on conviction on indictment, imprisonment for up to 5 years.
- **Section 3** — Unlawful interference with an information system.
- **Section 4** — Unlawful interception of information system communications.
- **Section 5** — Unlawful interference with data: destruction, damaging, deleting, deteriorating, altering or suppressing computer data without lawful authority.
- **Section 6** — Producing, supplying or possessing tools for committing the foregoing offences.

> *"A person who intentionally accesses, without lawful authority, the whole or any part of an information system is guilty of an offence."*
>
> Criminal Justice (Offences Relating to Information Systems) Act 2017, s. 2(1)

2.3 Copyright and Related Rights Act 2000 (Ireland)

The Copyright and Related Rights Act 2000 provides comprehensive protection for original literary, dramatic, musical and artistic works, as well as sound recordings, films, broadcasts and typographical arrangements. Educational recordings, lecture notes and slide presentations created by ICPS College constitute protected works.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

> *"Copyright is a property right and, subject to this Act, the owner of the copyright in a work shall have the exclusive right to undertake or authorise others to undertake all or any of the acts restricted by copyright."*
>
> Copyright and Related Rights Act 2000 (Ireland), s. 37(1)

Section 17 establishes the conditions for subsistence of copyright. Section 37 sets out the economic rights of the copyright owner, including the exclusive right to copy, distribute, communicate to the public, and make adaptations. Section 40 makes infringement a civil wrong; sections 140–141 create criminal liability for commercial-scale infringement.

2.4 Electronic Commerce Act 2000 (Ireland)

The Electronic Commerce Act 2000 provides the legal framework for electronic contracts, electronic signatures and electronic communications in Ireland. Section 9 establishes that information shall not be denied legal effect, validity or enforceability solely because it is in electronic form. Section 22 requires that electronic signatures used to sign documents of legal significance must satisfy defined criteria of reliability.

2.5 Freedom of Information Act 2014 (Ireland)

The Freedom of Information Act 2014 grants rights of access to records held by public bodies. While ICPS College as an accredited private provider does not ordinarily fall within the scope of FOI, its accrediting bodies and any public body that funds or inspects the College may be subject to FOI obligations. Section 35 creates a mandatory exemption for records that would disclose confidential information given to a public body in confidence. Section 37 protects personal information — access to records containing personal data is subject to data protection law.

2.6 Communications Regulation Acts 2002–2022 & ePrivacy Regulations

The ePrivacy Regulations 2011 (S.I. No. 336 of 2011, as amended) implement the EU ePrivacy Directive 2002/58/EC in Ireland. These Regulations govern the confidentiality of electronic communications, cookies and similar tracking technologies, unsolicited marketing communications, and the security of electronic communications networks. Regulation 5 provides that any interception of communications is unlawful without the consent of relevant parties.

> *"A person shall not use an electronic communications network to store information, or to gain access to information stored in the terminal equipment of a subscriber or user, unless the requirements of paragraph (2) are satisfied."*
>
> European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. 336/2011), Reg. 5(1)

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

2.7 Defamation Act 2009 (Ireland)

The Defamation Act 2009 governs the law of defamation in Ireland, abolishing the distinction between libel and slander. Section 6 defines a "defamatory statement" as a statement that tends to injure a person's reputation. A person who publishes a defamatory statement is liable in tort unless a defence such as truth (s. 16), absolute privilege (s. 17), qualified privilege (s. 18) or honest opinion (s. 20) applies. Sharing confidential communications from a college programme outside the group, where those communications make false or damaging assertions about identifiable individuals, could expose the disclosing party to defamation liability under this Act.

2.8 Employment Equality Acts 1998–2015 & Equal Status Acts 2000–2018

These Acts prohibit discrimination on nine protected grounds: gender; civil status; family status; age; disability; sexual orientation; race; religion; and membership of the Traveller community. In the educational context, any processing or disclosure of data that enables or results in discriminatory treatment contrary to the Equal Status Acts 2000–2018 will be both unlawful under equality legislation and potentially a breach of data protection law where the data concerned falls within special categories.

2.9 Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993

This Act regulates the lawful interception of postal packets and telecommunications messages by State authorities. Section 98 of the Post Office Act 1908 (as amended) makes the interception of telecommunications messages unlawful except where authorised by warrant. The Act predates modern digital communications but its principles inform subsequent cybercrime and data protection legislation.

2.10 Key Irish Case Law

Irish courts and the DPC have produced significant authority on privacy and data protection. The following cases are of particular importance:

- **Data Protection Commissioner v Facebook Ireland (High Court, 2020)** — The DPC sought High Court approval to refer questions to the CJEU concerning the legality of Standard Contractual Clauses for EU-US data transfers, leading to the landmark Schrems II judgment (C-311/18, 2020).
- **Nowak v Data Protection Commissioner [2016] IECA 301** — The Court of Appeal held that examination scripts constitute personal data of the candidate, confirmed on reference to the CJEU (C-434/16, [2017] EUECJ).
- **McDonald v Google Ireland Ltd [2021] IEHC 292** — The High Court examined the right to de-referencing in Irish proceedings, applying the Google Spain principles.
- **Kennedy v Limerick County Council [2020] IEHC 347** — Addressed legitimate interests as a basis for processing under GDPR in a public sector context.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

PART III — UNITED KINGDOM LAW

Following the UK's withdrawal from the European Union, the UK established its own data protection framework through the retained EU law mechanism. The UK GDPR and the Data Protection Act 2018 form the twin pillars of the UK framework. ICPS College, operating in Ireland, must be aware of UK law where it processes data of UK residents or maintains business relationships with UK organisations.

3.1 UK GDPR (Retained EU Law)

The UK GDPR is the GDPR as it has effect in domestic law pursuant to section 3 of the European Union (Withdrawal) Act 2018. It applies to processing carried out in the context of a UK establishment or processing personal data of individuals in the UK by controllers or processors offering goods/services or monitoring behaviour. The substantive provisions mirror those of the EU GDPR, including the seven principles, lawful bases, and data subject rights. Key divergences are emerging through the Data Protection and Digital Information Bill (pending at the time of writing).

3.2 Data Protection Act 2018 (United Kingdom)

The Data Protection Act 2018 (UK) supplements the UK GDPR by providing additional specification, exemptions and conditions. Part 2 applies the UK GDPR to most processing. Part 3 implements the Law Enforcement Directive (2016/680/EU) for processing by competent authorities. Part 4 applies modified data protection provisions to the intelligence services. The Information Commissioner's Office (ICO) is the supervisory authority under s. 115. Criminal offences include: unlawfully obtaining or disclosing personal data (s. 170); re-identification of de-identified data (s. 171); and alteration of personal data to prevent disclosure (s. 173).

> *“It is an offence for a person knowingly or recklessly to obtain or disclose personal data without the consent of the controller.”*
>
> Data Protection Act 2018 (UK), s. 170(1)

3.3 Computer Misuse Act 1990 (United Kingdom)

The Computer Misuse Act 1990 creates three core offences that are directly relevant to the unauthorised sharing of digital content and communications:

- **Section 1** — Unauthorised access to computer material: up to 2 years' imprisonment on conviction on indictment.
- **Section 2** — Unauthorised access with intent to commit or facilitate commission of further offences: up to 5 years' imprisonment.
- **Section 3** — Unauthorised acts with intent to impair or with recklessness as to impairing operation of a computer: up to 10 years' imprisonment.
- **Section 3A** (inserted by the Police and Justice Act 2006) — Making, supplying or obtaining articles for use in offences under ss. 1, 3 or 3ZA.
- **Section 3ZA** (inserted by the Serious Crime Act 2015) — Unauthorised acts causing or creating significant risk of serious damage of a material kind.

Suite 11241, 77 Sir John Rogerson’s Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

3.4 Copyright, Designs and Patents Act 1988 (United Kingdom)

The CDPA 1988 protects original literary, dramatic, musical, artistic works and secondary works. Section 1 establishes conditions for copyright subsistence; section 16 sets out the acts restricted by copyright. Unauthorised reproduction or communication to the public of lecture recordings or course materials is an infringement under s. 16(1). Section 107 creates criminal liability for commercial-scale infringement. The "communication right" under s. 20, inserted by the Copyright and Related Rights Regulations 2003, specifically covers digital transmission and streaming.

> *"Copyright in a work is infringed by a person who without the licence of the copyright owner does any of the acts restricted by the copyright."*
>
> Copyright, Designs and Patents Act 1988, s. 16(1)

3.5 Human Rights Act 1998 (United Kingdom)

The Human Rights Act 1998 gives domestic effect to the European Convention on Human Rights in UK law. Section 6 makes it unlawful for a public authority to act incompatibly with Convention rights, including Article 8 (right to private and family life). The Act has been applied extensively to privacy and data protection disputes in UK courts, including in the development of the tort of misuse of private information.

3.6 Investigatory Powers Act 2016 (United Kingdom)

The Investigatory Powers Act 2016 (the "Snoopers' Charter") consolidates and updates the legal framework for the interception of communications, equipment interference, data retention, and access to communications data by public authorities. Part 1, Chapter 1 prohibits the interception of communications in the course of transmission without a warrant or without the consent of parties to the communication. Unlawful interception is an offence under s. 3, carrying up to 2 years' imprisonment.

3.7 Online Safety Act 2023 (United Kingdom)

The Online Safety Act 2023 imposes duties on in-scope services to protect users from illegal and harmful content. Section 178 creates new criminal offences including: sharing intimate images without consent (s. 188); threatening communications (s. 181); and cyberflashing (s. 187). The Act gives Ofcom new powers to regulate online platforms and require the removal of harmful content.

3.8 Privacy and Electronic Communications Regulations 2003 (UK/PECR)

PECR 2003 (S.I. 2003/2426) implements the EU ePrivacy Directive in the UK. Regulation 6 requires informed consent before placing cookies on a user's device. Regulation 7 prohibits unsolicited marketing calls to subscribers registered with the Telephone Preference Service. Regulation 22 prohibits electronic mail marketing without prior consent.

3.9 Key UK Case Law

The following UK judgments are foundational in privacy and data protection law:

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

- **Campbell v MGN Ltd [2004] UKHL 22** — The House of Lords recognised the tort of misuse of private information as a distinct cause of action, establishing the reasonable expectation of privacy test.
- **Vidal-Hall v Google Inc [2015] EWCA Civ 311** — The Court of Appeal held that distress without financial loss is recoverable in data misuse claims.
- **Lloyd v Google LLC [2021] UKSC 50** — The Supreme Court held that loss of control of personal data alone does not constitute "damage" within the DPA 1998.
- **R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058** — The Court of Appeal found the police use of automated facial recognition technology unlawful for insufficient policy clarity.
- **WM Morrison Supermarkets plc v Various Claimants [2020] UKSC 12** — The Supreme Court held that an employer was not vicariously liable for an employee's deliberate disclosure of colleagues' payroll data.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

PART IV — EUROPEAN UNION LAW: GDPR & BEYOND

The European Union has developed the world's most comprehensive legal framework for data protection and digital rights. The GDPR is the centrepiece, but it is flanked by a rapidly expanding body of digital legislation. This Part surveys the key instruments in depth.

4.1 General Data Protection Regulation (EU) 2016/679 (GDPR) — Full Analysis

The GDPR, which entered into application on 25 May 2018, is a directly applicable regulation under Article 288 TFEU. It replaced the Data Protection Directive 95/46/EC and established a unified EU-wide data protection framework with extraterritorial reach under Article 3(2). Key structural elements:

- **Chapter I (Arts. 1–4)** — General provisions, material scope, territorial scope, and definitions.
- **Chapter II (Art. 5■1)** — Principles and lawful bases for processing.
- **Chapter III (Arts. 12–23)** — Data subject rights.
- **Chapter IV (Arts. 24–43)** — Controller and processor obligations, including DPIAs, DPOs, and security measures.
- **Chapter V (Arts. 44–49)** — International data transfers.
- **Chapter VI–VIII (Arts. 51–84)** — Supervisory authorities, cooperation mechanisms, remedies and penalties.

The maximum administrative fine under Article 83 GDPR is €20 million or 4% of total global annual turnover, whichever is higher, for the most serious infringements. Lower tier fines of €10 million or 2% of turnover apply to less serious infringements.

> *"Infringements of the following provisions shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher."*
>
> GDPR (EU) 2016/679, Article 83(5)

Article 32 GDPR requires controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including: pseudonymisation and encryption; ongoing confidentiality, integrity, availability and resilience of processing systems; ability to restore access to data in the event of an incident; and a process for regularly testing and evaluating the effectiveness of measures.

> *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."*
>
> GDPR (EU) 2016/679, Article 32(1)

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

4.1.1 Data Protection Impact Assessments (Article 35 GDPR)

A DPIA is mandatory where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, in particular where systematic and extensive evaluation of personal aspects of natural persons based on automated processing occurs; where large-scale processing of special category data takes place; or where there is systematic monitoring of a publicly accessible area on a large scale. Where a DPIA indicates high residual risk, prior consultation with the supervisory authority is required under Article 36.

4.2 ePrivacy Directive 2002/58/EC (as amended by 2009/136/EC)

The ePrivacy Directive governs the processing of personal data and the protection of privacy in the electronic communications sector. Article 5 provides that Member States shall ensure confidentiality of communications and the related traffic data. Article 5(3) requires informed consent before the storage of information on or retrieval from a user's terminal equipment. The proposed ePrivacy Regulation (COM(2017) 10 final) will replace the Directive.

> *"Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation."*
>
> ePrivacy Directive 2002/58/EC, Article 5(1)

4.3 NIS2 Directive (EU) 2022/2555

The Network and Information Security Directive 2 (NIS2) replaces NIS1 (Directive (EU) 2016/1148) and significantly expands the scope of cybersecurity obligations. Article 21 requires entities to adopt technical, operational and organisational measures commensurate with the risks posed to the security of network and information systems. These measures must include: risk analysis and information systems security policies; incident handling; business continuity and crisis management; supply chain security; security in network and information systems acquisition; training; cryptography and encryption; and multi-factor authentication. Member States must ensure that management bodies of essential and important entities approve the cybersecurity risk-management measures (Art. 20).

4.4 Digital Services Act (EU) 2022/2065

The DSA, which applies from 17 February 2024 for most providers, establishes a graduated liability framework for online intermediary services. Chapter II codifies conditions of exemption from liability for mere conduit, caching and hosting services. Chapter III imposes due diligence obligations including notice-and-action mechanisms, transparency reporting, content moderation measures, and advertisement repositories. Article 26 prohibits targeting advertising based on special category data under Article 9 GDPR.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

4.5 EU Artificial Intelligence Act (EU) 2024/1689

The AI Act, which entered into force on 1 August 2024, is the world's first comprehensive legal framework for artificial intelligence. It takes a risk-based approach: prohibited AI practices (Title II) include real-time remote biometric identification in public spaces; high-risk AI systems (Annex III) include those used in education and training, and employment and workers management; limited and minimal risk systems face transparency and other lighter obligations. Where ICPS College deploys AI-driven tools (e.g., adaptive learning systems, automated feedback), compliance obligations under the AI Act will apply.

4.6 Data Act (EU) 2023/2854

The Data Act, applicable from 12 September 2025, governs who may use and share data generated by connected products and related services. It introduces data access rights for users, portability rights, and restrictions on the use of non-personal data by cloud and edge services. Article 31 prohibits cloud providers from transferring non-personal data to non-EU jurisdictions that lack adequate protection.

4.7 Digital Operational Resilience Act (EU) 2022/2554 (DORA)

DORA, applicable from 17 January 2025, establishes a unified ICT risk management framework for financial entities and their ICT third-party service providers. While ICPS College is not a financial entity, any fintech or payment platform it uses must comply with DORA, which has implications for the resilience of payment data and third-party contracts.

4.8 EU Charter of Fundamental Rights

The Charter of Fundamental Rights of the European Union (2000/C 364/01), which has the same legal value as the EU Treaties since the Lisbon Treaty (Art. 6(1) TEU), contains foundational privacy and data protection rights:

> *"Article 7: Everyone has the right to respect for his or her private and family life, home and communications. Article 8: Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."*
>
> Charter of Fundamental Rights of the European Union, Arts. 7–8

4.9 Whistleblowing Directive (EU) 2019/1937

The Whistleblowing Directive protects persons who report breaches of EU law in the areas covered by the Directive (including data protection). Ireland implemented the Directive through the Protected Disclosures (Amendment) Act 2022. The Directive requires the establishment of internal and external reporting channels and prohibits retaliation against whistleblowers.

4.10 Key CJEU Case Law

The Court of Justice of the European Union has produced landmark data protection jurisprudence:

- **Google Spain (C-131/12) [2014]** — Established the right to de-referencing (the "right to be forgotten") in the context of search engine results. The Court held that search engines are data controllers and that links to outdated information may be removed on a data subject's request.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

- **Schrems I (C-362/14) [2015]** — Invalidated the EU-US Safe Harbour adequacy decision, fundamentally disrupting transatlantic data flows and emphasising that third-country adequacy requires essentially equivalent protection.
- **Schrems II (C-311/18) [2020]** — Invalidated the EU-US Privacy Shield adequacy decision and upheld SCCs subject to a case-by-case transfer impact assessment obligation.
- **Digital Rights Ireland (C-293/12) [2014]** — Invalidated Directive 2006/24/EC on blanket data retention, holding that indiscriminate retention of communications data violated Articles 7 and 8 of the Charter.
- **Fashion ID (C-40/17) [2019]** — Held that embedding third-party social plugins (Facebook Like buttons) on a website makes the site operator a joint controller for the collection and transmission phase.
- **Meta / WhatsApp (C-252/21) [2023]** — The CJEU clarified that a supervisory authority may find an infringement of competition law based on a breach of GDPR obligations in the context of market dominance.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

PART V — INTERNATIONAL & COMPARATIVE LAW

Beyond Irish, UK and EU law, a body of international law, conventions and standards governs the protection of personal data, the confidentiality of communications, and the security of information systems.

5.1 European Convention on Human Rights, Article 8

Article 8 of the ECHR protects the right to respect for private and family life, home and correspondence. Interferences must be (i) in accordance with the law; (ii) in pursuance of a legitimate aim (listed in Art. 8(2)); and (iii) necessary in a democratic society. The ECtHR has developed a rich body of case law applying Article 8 to data processing, surveillance, employment monitoring, and the disclosure of confidential information.

> *"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*
>
> European Convention on Human Rights (1950), Article 8(2)

- **S and Marper v UK [2008] ECHR 1581** — Grand Chamber held that indefinite retention of DNA and fingerprints of acquitted persons breached Article 8.
- **Barbulescu v Romania [2017] ECHR 742 (GC)** — Grand Chamber established a test for the proportionality of employer monitoring of employees' electronic communications.
- **López Ribalda v Spain [2019] ECHR 879 (GC)** — Grand Chamber found secret video surveillance of employees in supermarkets not a breach of Art. 8 where based on reasonable suspicion of theft.
- **Copland v UK [2007] ECHR 253** — ECtHR held that covert monitoring of telephone, email and internet usage of an employee without knowledge breached Article 8.

5.2 Council of Europe Convention 108 & Convention 108+ (2018)

Convention 108 (1981) was the first legally binding international instrument on data protection. It requires Parties to ensure that personal data are processed in conformity with core principles of quality, sensitive data protection, security, and respect for data subject rights. Convention 108+ (the 2018 modernising Protocol) updates these obligations, introducing: mandatory notification of data breaches; strengthened supervisory authority independence; proportionality requirements for sensitive data processing; and specific protections for children.

> *"Personal data undergoing automatic processing shall be: obtained and processed fairly and lawfully; stored for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored; accurate and, where necessary, kept up to date; preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."*
>
> Council of Europe Convention 108 (1981), Article 5

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

5.3 Budapest Convention on Cybercrime (2001)

The Convention on Cybercrime (CETS No. 185), concluded in Budapest on 23 November 2001, is the first international treaty seeking to address internet and computer crime by harmonising national laws, improving investigative techniques, and increasing cooperation among nations. Chapter II, Section 1 creates offences against the confidentiality, integrity and availability of computer data and systems, including: illegal access (Art. 2); illegal interception (Art. 3); data interference (Art. 4); system interference (Art. 5); and misuse of devices (Art. 6). The Second Additional Protocol (2022) enhances cross-border access to subscriber information and emergency production orders.

5.4 Universal Declaration of Human Rights (1948), Article 12

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*
>
> Universal Declaration of Human Rights (1948), Article 12

5.5 International Covenant on Civil and Political Rights (1966), Article 17

The ICCPR, ratified by Ireland, provides in Article 17 that: (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; (2) Everyone has the right to the protection of the law against such interference or attacks. The UN Human Rights Committee's General Comment No. 16 (1988) elaborates that the right to privacy in electronic communications extends to the content and metadata of messages.

5.6 OECD Privacy Guidelines (1980, Revised 2013)

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, revised 2013) established eight privacy principles that influenced data protection law globally: collection limitation; data quality; purpose specification; use limitation; security safeguards; openness; individual participation; and accountability. The 2013 revision added a national privacy strategy requirement and data breach notification.

5.7 ISO/IEC 27001:2022 and ISO/IEC 27701:2019

ISO/IEC 27001:2022 (Information Security Management Systems — Requirements) is the internationally recognised standard for establishing, implementing, maintaining and continually improving an information security management system (ISMS). It requires a risk treatment process addressing confidentiality, integrity and availability. ISO/IEC 27701:2019 (Privacy Information Management Systems) extends ISO/IEC 27001/27002 to include requirements and guidance for establishing a Privacy Information Management System (PIMS) and acts as a GDPR compliance implementation guide.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

5.8 APEC Privacy Framework (2004, Revised 2015)

The Asia-Pacific Economic Cooperation Privacy Framework applies nine principles: preventing harm; notice; collection limitation; uses of personal information; choice; integrity of personal information; security safeguards; access and correction; and accountability. The Cross-Border Privacy Rules (CBPR) system is the APEC enforcement mechanism for international transfers.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

PART VI — APPLICATION TO ICPS COLLEGE

This Part translates the legal framework set out in Parts I–V into concrete obligations for ICPS College in its capacity as a data controller, educational provider, and CPD Standards Office accredited institution.

6.1 Learner Data — Collection, Processing & Retention

ICPS College collects and processes a range of learner personal data, including identification data; contact information; enrolment and payment records; assessment results and feedback; and, where relevant, clinical supervision records that may include health-related information (special category data under Article 9 GDPR). The College's lawful basis for processing enrolment and assessment data is primarily contract (Art. 6(1)(b) GDPR) and legal obligation (Art. 6(1)(c)). Where health-related clinical information is recorded, explicit consent (Art. 9(2)(a)) or substantial public interest in the context of professional training (Art. 9(2)(j)) provide the legal basis.

The College's minimum seven-year retention period for assessment records (consistent with accreditation obligations) must be balanced against the storage limitation principle. Where data is retained beyond programme completion, the College must ensure a documented purpose and proportionality justification.

6.2 Confidentiality of Communications — All Channels

All communications within ICPS College-facilitated environments — whether via the Moodle learning management system, video conferencing platforms, email, group messaging, discussion forums, or in-person sessions — are confidential. No participant, staff member or third party may disclose the content of communications to persons outside the relevant group without the prior written consent of the College and, where appropriate, all relevant parties. This obligation is grounded in:

- ◆ GDPR Article 5(1)(f) — integrity and confidentiality of personal data.
- ◆ ePrivacy Regulations — confidentiality of electronic communications.
- ◆ Article 8 ECHR — reasonable expectation of privacy in correspondence.
- ◆ Convention 108 Article 7 — security safeguards for personal data.
- ◆ Professional ethics obligations of the counselling and psychotherapy field.

6.3 Recorded Lectures and Educational Content — Prohibition on Sharing

All lecture recordings, instructional videos, webinar recordings, slides, handouts and course materials produced by or on behalf of ICPS College are the exclusive intellectual property of the College, protected under the Copyright and Related Rights Act 2000 (Ireland), the CDPA 1988 (UK), and the InfoSoc Directive (EU) 2001/29/EC. Sharing, uploading, distributing, posting or otherwise communicating this content beyond the enrolled participant group is strictly prohibited and may result in:

- ◆ Civil proceedings for copyright infringement (s. 37 CRRA 2000; s. 16 CDPA 1988).
- ◆ Criminal liability for commercial-scale infringement (s. 140 CRRA 2000; s. 107 CDPA 1988).
- ◆ Breach of contract (terms and conditions of enrolment).
- ◆ Data protection liability where recordings capture personal data of other participants (GDPR Arts. 5, 6, 32).
- ◆ Referral to the relevant professional body and potential impact on professional registration.
- ◆ Immediate withdrawal from the programme.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

6.4 Data Breach Procedures

In the event of a personal data breach, the College must assess the risk to data subjects' rights and freedoms. Where the breach is likely to result in a risk, notification must be made to the DPC within 72 hours of becoming aware (GDPR Art. 33). Where the breach is likely to result in a high risk, notification must also be made to affected data subjects without undue delay (GDPR Art. 34). The College must maintain a record of all breaches, including those not reported to the DPC, pursuant to GDPR Art. 33(5).

6.5 Data Subject Rights in Practice

Learners and staff may exercise their rights under GDPR Chapter III. All requests must be acknowledged within 5 working days and fulfilled within one calendar month. The College must verify the identity of the requestor before disclosure. Access requests should be satisfied in structured, commonly used format. Where the right to erasure is exercised, the College must assess competing obligations (e.g., retention for accreditation audit) before effecting deletion.

Suite 11241, 77 Sir John Rogerson’s Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

PART VII — KEY LEGAL QUOTATIONS & STATUTORY EXTRACTS

This Part compiles the most important statutory and judicial quotations relevant to the confidentiality, data protection and legal notice obligations of ICPS College. These extracts should be read in the context of the fuller provisions set out in Parts I–VI above.

Accountability — Controller Obligations

> *"The controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."*
>
> GDPR (EU) 2016/679, Article 24(1)

Processor Obligations

> *"A processor shall not engage another processor without prior specific or general written authorisation of the controller."*
>
> GDPR (EU) 2016/679, Article 28(2)

International Transfers

> *"Any transfer of personal data to a third country or an international organisation shall only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor."*
>
> GDPR (EU) 2016/679, Article 44

Irish Cybercrime Offence

> *"A person who intentionally and without lawful excuse accesses, or causes a computer to access, any information contained in a computer is guilty of an offence."*
>
> Criminal Justice (Offences Relating to Information Systems) Act 2017 (Ireland), s. 2(1) (paraphrased)

Copyright Ownership

> *"Copyright is a property right and, subject to this Act, the owner of the copyright in a work shall have the exclusive right to undertake or authorise others to undertake all or any of the acts restricted by copyright."*
>
> Copyright and Related Rights Act 2000 (Ireland), s. 37(1)

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

Integrity and Confidentiality Principle

> *"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage."*
>
> GDPR (EU) 2016/679, Article 5(1)(f)

Right to Privacy

> *"Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society."*
>
> European Convention on Human Rights (1950), Articles 8(1)–8(2)

UK Data Misuse Offence

> *"It is an offence for a person knowingly or recklessly to obtain or disclose personal data without the consent of the controller."*
>
> Data Protection Act 2018 (UK), s. 170(1)

International Human Rights

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."*
>
> Universal Declaration of Human Rights (1948), Article 12

Purpose Limitation — International Framework

> *"Personal data undergoing automatic processing shall be: stored for specified and legitimate purposes and not used in a way incompatible with those purposes."*
>
> Council of Europe Convention 108 (1981), Article 5(b)

Breach Notification Threshold

> *"Where the supervisory authority considers that a personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, it need not be notified to the supervisory authority."*
>
> GDPR (EU) 2016/679, Article 33(1) (a contrario)

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

Right t Erasure

Welcome to ICPS College

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

PART VIII — LEGAL REFERENCES: 200 CITATIONS

The following 200 references are provided in alphabetical and categorical order, spanning primary Irish legislation, UK primary legislation, European Union regulations and directives, Council of Europe and international conventions, CJEU and ECHR case law, UK and Irish case law, regulatory guidance documents, international standards frameworks, and academic sources. All references are cited in accordance with OSCOLA / Harvard hybrid conventions appropriate to a mixed legal and academic document.

Primary Irish Legislation [1–20]

[1] Data Protection Act 2018 (Ireland). Number 7 of 2018. Dublin: Stationery Office.

[2] Data Sharing and Governance Act 2019 (Ireland). Number 5 of 2019. Dublin: Stationery Office.

[3] Criminal Justice (Offences Relating to Information Systems) Act 2017 (Ireland). Number 2 of 2017. Dublin: Stationery Office.

[4] Copyright and Related Rights Act 2000 (Ireland). Number 28 of 2000. Dublin: Stationery Office.

[5] Electronic Commerce Act 2000 (Ireland). Number 27 of 2000. Dublin: Stationery Office.

[6] Communications Regulation Act 2002 (Ireland). Number 20 of 2002. Dublin: Stationery Office.

[7] Defamation Act 2009 (Ireland). Number 31 of 2009. Dublin: Stationery Office.

[8] Freedom of Information Act 2014 (Ireland). Number 30 of 2014. Dublin: Stationery Office.

[9] Freedom of Information Act 1997 (Ireland). Number 13 of 1997. Dublin: Stationery Office.

[10] Education Act 1998 (Ireland). Number 51 of 1998. Dublin: Stationery Office.

[11] Health Act 2004 (Ireland). Number 42 of 2004. Dublin: Stationery Office.

[12] Employment Equality Act 1998 (Ireland). Number 21 of 1998. Dublin: Stationery Office.

[13] Equal Status Act 2000 (Ireland). Number 8 of 2000. Dublin: Stationery Office.

[14] Civil Liability Act 1961 (Ireland). Number 41 of 1961. Dublin: Stationery Office.

[15] Non-Fatal Offences Against the Person Act 1997 (Ireland). Number 26 of 1997. Dublin: Stationery Office.

[16] Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 (Ireland). Number 10 of 1993. Dublin: Stationery Office.

[17] Criminal Damage Act 1991 (Ireland). Number 31 of 1991. Dublin: Stationery Office.

[18] Protected Disclosures (Amendment) Act 2022 (Ireland). Number 27 of 2022. Dublin: Stationery Office.

[19] Broadcasting Act 2009 (Ireland). Number 18 of 2009. Dublin: Stationery Office.

[20] Consumer Protection Act 2007 (Ireland). Number 19 of 2007. Dublin: Stationery Office.

UK Primary Legislation [21–40]

[21] Data Protection Act 2018 (UK). c. 12. London: The Stationery Office.

[22] European Union (Withdrawal) Act 2018 (UK). c. 16. London: The Stationery Office. [Retaining EU GDPR as UK GDPR].

[23] Computer Misuse Act 1990 (UK). c. 18. London: The Stationery Office.

[24] Copyright, Designs and Patents Act 1988 (UK). c. 48. London: The Stationery Office.

[25] Human Rights Act 1998 (UK). c. 42. London: The Stationery Office.

[26] Freedom of Information Act 2000 (UK). c. 36. London: The Stationery Office.

[27] Environmental Information Regulations 2004 (UK). SI 2004/3391. London: The Stationery Office.

[28] Regulation of Investigatory Powers Act 2000 (UK). c. 23. London: The Stationery Office.

[29] Investigatory Powers Act 2016 (UK). c. 25. London: The Stationery Office.

[30] Online Safety Act 2023 (UK). c. 50. London: The Stationery Office.

[31] Equality Act 2010 (UK). c. 15. London: The Stationery Office.

[32] Electronic Communications Act 2000 (UK). c. 7. London: The Stationery Office.

Suite 11241, 77 Sir John Rogerson’s Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

[33] Privacy and Electronic Communications Regulations 2003 (UK). SI 2003/2426. London: The Stationery Office.

[34] Network and Information Systems Regulations 2018 (UK). SI 2018/506. London: The Stationery Office.

[35] Serious Crime Act 2015 (UK). c. 9. London: The Stationery Office.

[36] Digital Economy Act 2017 (UK). c. 30. London: The Stationery Office.

[37] Malicious Communications Act 1988 (UK). c. 27. London: The Stationery Office.

[38] Defamation Act 2013 (UK). c. 26. London: The Stationery Office.

[39] Police and Justice Act 2006 (UK). c. 48. London: The Stationery Office.

[40] Official Secrets Act 1989 (UK). c. 6. London: The Stationery Office.

EU Regulations & Directives [41–70]

[41] European Parliament and Council (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (GDPR). Official Journal of the European Union, L 119, pp. 1–88.

[42] European Parliament and Council (2002). Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive). OJ L 201.

[43] European Parliament and Council (2009). Directive 2009/136/EC amending the ePrivacy Directive. OJ L 337.

[44] European Parliament and Council (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). OJ L 333.

[45] European Parliament and Council (2022). Regulation (EU) 2022/2065 on a Single Market For Digital Services (Digital Services Act). OJ L 277.

[46] European Parliament and Council (2022). Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act). OJ L 265.

[47] European Parliament and Council (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act). OJ L.

[48] European Parliament and Council (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). OJ L 333.

[49] European Parliament and Council (2016). Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities (Law Enforcement Directive). OJ L 119.

[50] European Parliament and Council (2014). Regulation (EU) 910/2014 on electronic identification and trust services (eIDAS). OJ L 257.

[51] European Parliament and Council (2019). Regulation (EU) 2019/881 on ENISA and cybersecurity certification (Cybersecurity Act). OJ L 151.

[52] European Parliament and Council (2019). Directive (EU) 2019/1937 on the protection of persons reporting breaches of Union law (Whistleblowing Directive). OJ L 305.

[53] European Parliament and Council (2019). Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market. OJ L 130.

[54] European Parliament and Council (2001). Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive). OJ L 167.

[55] European Parliament and Council (2000). Directive 2000/31/EC on certain legal aspects of information society services (e-Commerce Directive). OJ L 178.

[56] European Parliament and Council (1996). Directive 96/9/EC on the legal protection of databases. OJ L 77.

[57] European Parliament and Council (2023). Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act). OJ L.

[58] European Parliament and Council (2022). Regulation (EU) 2022/868 on European data governance (Data Governance Act). OJ L 152.

[59] European Parliament and Council (2022). Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive). OJ L 333.

[60] European Parliament and Council (2017). Directive (EU) 2017/541 on combating terrorism. OJ L 88.

[61] Council of the European Union (2013). Directive 2013/40/EU on attacks against information systems. OJ L 218.

[62] European Parliament and Council (2006). Directive 2006/24/EC on data retention [Invalidated by CJEU in Digital Rights Ireland, C-293/12]. OJ L 105.

[63] European Parliament and Council (2016). Directive (EU) 2016/1148 on security of network and information systems (NIS1 Directive). OJ L 194.

[64] European Parliament and Council (2015). Directive (EU) 2015/2366 on payment services in the internal market (PSD2). OJ L 337.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

[65] European Parliament and Council (2018). Directive (EU) 2018/843 amending AML Directive. OJ L 156.

[66] European Parliament and Council (2015). Regulation (EU) 2015/847 on information accompanying transfers of funds. OJ L 141.

[67] European Parliament and Council (2011). Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children. OJ L 335.

[68] Charter of Fundamental Rights of the European Union (2000). OJ C 364/01.

[69] European Commission (2017). Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation Proposal). COM(2017) 10 final.

[70] European Commission (2021). Proposal for a European Health Data Space Regulation. COM(2021) 799 final.

Council of Europe & International Conventions [71–90]

[71] Council of Europe (1950). Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights). CETS No. 005. Rome.

[72] Council of Europe (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). CETS No. 108. Strasbourg.

[73] Council of Europe (2018). Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108+). CETS No. 223. Strasbourg.

[74] Council of Europe (2001). Convention on Cybercrime (Budapest Convention). CETS No. 185. Budapest.

[75] Council of Europe (2003). Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature. CETS No. 189.

[76] Council of Europe (2022). Second Additional Protocol to the Convention on Cybercrime (E-evidence). CETS No. 224. Strasbourg.

[77] Council of Europe (1961). European Social Charter. CETS No. 035. Turin.

[78] Council of Europe (2005). Convention on the Prevention of Terrorism. CETS No. 196. Warsaw.

[79] Council of Europe (2007). Convention on Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). CETS No. 201.

[80] United Nations (1948). Universal Declaration of Human Rights. Adopted by General Assembly Resolution 217A(III), 10 December 1948. Paris.

[81] United Nations (1966). International Covenant on Civil and Political Rights. UNTS Vol. 999, p. 171. New York.

[82] United Nations (1966). International Covenant on Economic, Social and Cultural Rights. UNTS Vol. 993, p. 3. New York.

[83] United Nations (1989). Convention on the Rights of the Child. UNTS Vol. 1577, p. 3. New York.

[84] United Nations (2003). United Nations Convention Against Corruption (UNCAC). UNTS Vol. 2349. New York.

[85] United Nations Human Rights Committee (1988). General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17). New York: UNHRC.

[86] OECD (1980, revised 2013). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD Publishing.

[87] APEC (2004, revised 2015). APEC Privacy Framework. Singapore: APEC Secretariat.

[88] African Union (2014). Convention on Cyber Security and Personal Data Protection (Malabo Convention). Addis Ababa: African Union.

[89] Commonwealth Secretariat (2017). Commonwealth Cybercrime Initiative Model Law. London: Commonwealth Secretariat.

[90] United Nations Human Rights Council (2014). The Right to Privacy in the Digital Age. Resolution A/HRC/RES/26/13. Geneva: UNHRC.

Court of Justice of the EU (CJEU) Case Law [91–110]

[91] Google Spain SL and Google Inc v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez (C-131/12) [2014] EUECJ. ECLI:EU:C:2014:317.

[92] Maximillian Schrems v Data Protection Commissioner (Schrems I) (C-362/14) [2015] EUECJ. ECLI:EU:C:2015:650.

[93] Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems II) (C-311/18) [2020] EUECJ. ECLI:EU:C:2020:559.

[94] Bodil Lindqvist v Aklagarkammaren i Jonkoping (C-101/01) [2003] EUECJ. ECLI:EU:C:2003:596.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

[95] Digital Rights Ireland Ltd v Minister for Communications (C-293/12) [2014] EUECJ. ECLI:EU:C:2014:238.

[96] Tele2 Sverige AB v Post-och telestyrelsen (C-203/15) [2016] EUECJ. ECLI:EU:C:2016:970.

[97] Weltimmo s.r.o. v Nemzeti Adatvedelmi es Informacioszabadsag Hatosag (C-230/14) [2015] EUECJ. ECLI:EU:C:2015:639.

[98] Patrick Breyer v Bundesrepublik Deutschland (C-582/14) [2016] EUECJ. ECLI:EU:C:2016:779.

[99] Osterreichischer Rundfunk and Others (C-465/00) [2003] EUECJ. ECLI:EU:C:2003:294.

[100] Volker und Markus Schecke GbR v Land Hessen (C-92/09) [2010] EUECJ. ECLI:EU:C:2010:662.

[101] YS and Others v Minister voor Immigratie, Integratie en Asiel (C-141/12) [2014] EUECJ. ECLI:EU:C:2014:2081.

[102] Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (C-40/17) [2019] EUECJ. ECLI:EU:C:2019:629.

[103] Orange Romania SA v Autoritatea Nationala de Supraveghere a Prelucrarii Datelor (C-61/19) [2020] EUECJ. ECLI:EU:C:2020:901.

[104] Meta Platforms and Others (Bundeskartellamt) (C-252/21) [2023] EUECJ. ECLI:EU:C:2023:537.

[105] TU and RE v Google LLC (C-460/20) [2022] EUECJ. ECLI:EU:C:2022:962.

[106] IAB Europe v Gegevensbeschermingsautoriteit (C-604/22) [2024] EUECJ.

[107] Peter Nowak v Data Protection Commissioner (C-434/16) [2017] EUECJ. ECLI:EU:C:2017:994.

[108] Rigas satiksme (C-13/16) [2017] EUECJ. ECLI:EU:C:2017:336.

[109] SRB v EDPS (T-557/20) [2021] EU:T:2021:767.

[110] GC and Others v CNIL (C-136/17) [2019] EUECJ. ECLI:EU:C:2019:773.

European Court of Human Rights (ECtHR) Case Law [111–120]

[111] Rotaru v Romania [2000] ECHR 192. Application No. 28341/95. Strasbourg: ECtHR.

[112] Amann v Switzerland [2000] ECHR 87. Application No. 27798/95. Strasbourg: ECtHR.

[113] Peck v United Kingdom [2003] ECHR 44. Application No. 44647/98. Strasbourg: ECtHR.

[114] S and Marper v United Kingdom [2008] ECHR 1581. Application Nos. 30562/04 and 30566/04. Strasbourg: ECtHR (Grand Chamber).

[115] Barbulescu v Romania [2017] ECHR 742. Application No. 61496/08. Strasbourg: ECtHR (Grand Chamber).

[116] Lopez Ribalda and Others v Spain [2019] ECHR 879. Application Nos. 1874/13 and 8567/13. Strasbourg: ECtHR (Grand Chamber).

[117] Copland v United Kingdom [2007] ECHR 253. Application No. 62617/00. Strasbourg: ECtHR.

[118] K.U. v Finland [2008] ECHR 1526. Application No. 2872/02. Strasbourg: ECtHR.

[119] Uzun v Germany [2010] ECHR 2031. Application No. 35623/05. Strasbourg: ECtHR.

[120] Big Brother Watch and Others v United Kingdom [2021] ECHR. Application No. 58170/13. Strasbourg: ECtHR (Grand Chamber).

UK Case Law [121–130]

[121] Campbell v MGN Limited [2004] UKHL 22. [2004] 2 AC 457.

[122] Durant v Financial Services Authority [2003] EWCA Civ 1746. [2004] FSR 28.

[123] Vidal-Hall v Google Inc [2015] EWCA Civ 311. [2016] QB 1003.

[124] NT1 and NT2 v Google LLC [2018] EWHC 799 (QB). [2018] 3 WLR 1165.

[125] Gulati v MGN Limited [2015] EWCA Civ 1291. [2017] QB 149.

[126] Lloyd v Google LLC [2021] UKSC 50. [2022] AC 1217.

[127] WM Morrison Supermarkets plc v Various Claimants [2020] UKSC 12. [2020] AC 989.

[128] R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058. [2020] 1 WLR 5037.

[129] Richard v BBC [2018] EWHC 1837 (Ch). [2019] Ch 169.

[130] Common Services Agency v Scottish Information Commissioner [2008] UKHL 47. [2008] 1 WLR 1550.

Irish Case Law [131–140]

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

[131] Data Protection Commissioner v Facebook Ireland Limited (High Court, 2020). [2020] IEHC 559.

[132] Nowak v Data Protection Commissioner [2016] IECA 301.

[133] McDonald v Google Ireland Limited [2021] IEHC 292.

[134] Kennedy v Limerick County Council [2020] IEHC 347.

[135] Ryanair Ltd v Data Protection Commissioner [2002] IEHC 54.

[136] Data Protection Commissioner — Decision re: WhatsApp Ireland Ltd (DPC Inquiry Reference IN-18-5-5, 2021).

[137] Dokie v Garda National Immigration Bureau [2011] IEHC 48.

[138] Towey v Minister for Justice, Equality and Law Reform [2004] IEHC 258.

[139] Minister for Justice, Equality and Law Reform v Bailey (Supreme Court, 2012) [2012] IESC 16.

[140] Data Protection Commissioner — Annual Report 2023 (enforcement actions and decisions summary). Dublin: DPC.

Regulatory Guidance & Decisions [141–160]

[141] European Data Protection Board (2022). Guidelines 01/2022 on Data Subject Rights — Right of Access. Version 2.0. Brussels: EDPB.

[142] European Data Protection Board (2022). Guidelines 02/2022 on the Application of Article 60 GDPR. Brussels: EDPB.

[143] European Data Protection Board (2022). Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement. Brussels: EDPB.

[144] European Data Protection Board (2020). Guidelines 05/2020 on Consent under Regulation 2016/679. Version 1.1. Brussels: EDPB.

[145] European Data Protection Board (2022). Guidelines 03/2022 on Dark Patterns in Social Media Platform Interfaces. Brussels: EDPB.

[146] European Data Protection Board (2019). Guidelines 01/2019 on Codes of Conduct and Monitoring Bodies. Brussels: EDPB.

[147] European Data Protection Board (2019). Guidelines 4/2019 on Article 25 — Data Protection by Design and by Default. Brussels: EDPB.

[148] European Data Protection Board (2019). Guidelines 2/2019 on Personal Data Processing under Article 6(1)(b) GDPR. Brussels: EDPB.

[149] European Data Protection Board (2018). Guidelines on Transparency under Regulation 2016/679. WP260 Rev.01. Brussels: EDPB.

[150] European Data Protection Board (2018). Guidelines on Personal Data Breach Notification. WP250 Rev.01. Brussels: EDPB.

[151] European Data Protection Board (2020). Recommendations 01/2020 on Measures that Supplement Transfer Tools. Brussels: EDPB.

[152] Article 29 Working Party (2016). Guidelines on Data Protection Officers. WP243 Rev.01. Brussels: Art. 29 WP.

[153] Article 29 Working Party (2013). Opinion 03/2013 on Purpose Limitation. WP203. Brussels: Art. 29 WP.

[154] Data Protection Commission, Ireland (2021). Guidance on Legitimate Interests as a Legal Basis. Dublin: DPC.

[155] Data Protection Commission, Ireland (2023). Guidance on Children's Personal Data. Dublin: DPC.

[156] Data Protection Commission, Ireland (2022). Guidance on Research and GDPR. Dublin: DPC.

[157] Information Commissioner's Office (2024). Guide to the UK GDPR — Lawful Basis for Processing. Wilmslow: ICO.

[158] Information Commissioner's Office (2023). Guidance on AI and Data Protection. Wilmslow: ICO.

[159] Information Commissioner's Office (2021). Age Appropriate Design: A Code of Practice for Online Services. Wilmslow: ICO.

[160] European Data Protection Supervisor (2021). Opinion on the Proposal for the Artificial Intelligence Act. Brussels: EDPS.

International Standards & Frameworks [161–175]

[161] International Organisation for Standardisation (2022). ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva: ISO.

[162] International Organisation for Standardisation (2019). ISO/IEC 27701:2019 — Security Techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management. Geneva: ISO.

[163] International Organisation for Standardisation (2022). ISO/IEC 27002:2022 — Information Security, Cybersecurity and Privacy Protection — Information Security Controls. Geneva: ISO.

[164] International Organisation for Standardisation (2018). ISO/IEC 29101:2018 — Privacy Architecture Framework. Geneva: ISO.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

[165] International Organisation for Standardisation (2017). ISO/IEC 29134:2017 — Guidelines for Privacy Impact Assessment. Geneva: ISO.

[166] International Organisation for Standardisation (2020). ISO/IEC 29184:2020 — Online Privacy Notices and Consent. Geneva: ISO.

[167] National Institute of Standards and Technology (2020). NIST Privacy Framework v1.0: A Tool for Improving Privacy through Enterprise Risk Management. Gaithersburg, MD: NIST.

[168] National Institute of Standards and Technology (2024). NIST Cybersecurity Framework v2.0. Gaithersburg, MD: NIST.

[169] National Institute of Standards and Technology (2020). NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organisations. Gaithersburg, MD: NIST.

[170] European Union Agency for Cybersecurity (ENISA) (2019). Pseudonymisation Techniques and Best Practices. Heraklion: ENISA.

[171] European Union Agency for Cybersecurity (ENISA) (2020). Guidelines for Securing the Internet of Things. Heraklion: ENISA.

[172] European Union Agency for Cybersecurity (ENISA) (2023). ENISA Threat Landscape 2023. Heraklion: ENISA.

[173] European Union Agency for Cybersecurity (ENISA) (2020). Guidelines on Security Measures under the GDPR. Heraklion: ENISA.

[174] Cloud Security Alliance (2021). Cloud Controls Matrix (CCM) v4.0. Seattle, WA: CSA.

[175] Center for Internet Security (2021). CIS Controls v8. East Greenbush, NY: CIS.

Academic References [176–195]

[176] Bygrave, L.A. (2014) Data Privacy Law: An International Perspective. Oxford: Oxford University Press.

[177] Kuner, C. (2013) Transborder Data Flows and Data Privacy Law. Oxford: Oxford University Press.

[178] Voigt, P. and von dem Bussche, A. (2017) The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer.

[179] Carey, P. (2018) Data Protection: A Practical Guide to UK and EU Law. 5th edn. Oxford: Oxford University Press.

[180] Moreham, N.A. and Warby, M. (eds.) (2019) Tugendhat and Christie: The Law of Privacy and the Media. 3rd edn. Oxford: Oxford University Press.

[181] Solove, D.J. (2008) Understanding Privacy. Cambridge, MA: Harvard University Press.

[182] Westin, A.F. (1967) Privacy and Freedom. New York: Atheneum.

[183] Nissenbaum, H. (2010) Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press.

[184] Erdos, D. (2016) European Union Data Protection Law and Media Expression. Oxford: Oxford University Press.

[185] Swire, P. and Ahmad, K. (2012) Foundations of Information Privacy and Data Protection. Portsmouth, NH: IAPP.

[186] Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015) 'Privacy and human behavior in the age of information.' Science, 347(6221), pp. 509–514.

[187] Zarsky, T.Z. (2017) 'Incompatible: The GDPR in the Age of Big Data.' Seton Hall Law Review, 47(4), pp. 995–1020.

[188] Wachter, S., Mittelstadt, B. and Russell, C. (2017) 'Counterfactual Explanations Without Opening the Black Box.' Harvard Journal of Law & Technology, 31(2).

[189] Binns, R. (2018) 'Algorithmic Accountability and Public Reason.' Philosophy & Technology, 31(4), pp. 543–556.

[190] Clarke, R. (1988) 'Information Technology and Dataveillance.' Communications of the ACM, 31(5), pp. 498–512.

[191] Holvast, J. (2009) 'History of Privacy.' IFIP Advances in Information and Communication Technology, 298, pp. 13–42.

[192] Ball, K. (2009) 'Exposure: Exploring the subject of surveillance.' Information, Communication & Society, 12(5), pp. 639–657.

[193] Bygrave, L.A. and Bing, J. (eds.) (2009) Internet Governance: Infrastructure and Institutions. Oxford: Oxford University Press.

[194] Korff, D. (2010) Data Protection Laws in the European Union. 2nd edn. New York: Federation of European Direct and Interactive Marketing (FEDMA) / ICC.

[195] Purtova, N. (2018) 'The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law.' Law, Innovation and Technology, 10(1), pp. 40–81.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie

Regulatory & CPD Sources [196–200]

[196] GDPR (EU) 2016/679, Article 9 — Processing of Special Categories of Personal Data. Official Journal of the European Union, L 119, pp. 1–88.

[197] GDPR (EU) 2016/679, Recital 51 — Sensitive personal data deserving higher protection, including health data and special category data.

[198] Data Protection Commission, Ireland (2020). Guidance on the Processing of Health Data. Dublin: DPC.

[199] European Data Protection Board (2020). Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak. Brussels: EDPB.

[200] CPD Standards Office (2023). Data Protection and Privacy Policy Framework for CPD Standards Office Accredited Providers. Provider No. PDCD1110. London: CPD Standards Office.

Suite 11241, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5 • Tel: 01 963 6141 • Freephone: 1800 681 456 • education@icps.ie • www.icps.ie