ICPHAA

Irish Counselling, Psychotherapy & Allied Healthcare Professionals Association

REGULATION, LAW & DATA PROTECTION

Legal & Data Governance Policy

How ICPHAA processes personal data lawfully, fairly and securely as a data controller, and what members must do as data controllers for their own client records.

REFERENCE	ICPHAA-POL-26	VERSION	1.0
EFFECTIVE	9 November 2026	NEXT REVIEW	9 November 2027
POLICY OWNER	ICPHAA Board of Directors		

Irish Counselling, Psychotherapy & Allied Healthcare Professionals Association

A voluntary, not-for-profit professional association · admin@icphaa.ie · www.icphaa.ie
Policy and procedure framework of the Association · ICPHAA-POL-26

REGULATION, LAW & DATA PROTECTION · ICPHAA-POL-26

Legal & Data Governance Policy

APPLIES TO	The ICPHAA Board, Registry, Accreditation Department, staff, volunteers and processors, and every member as controller of their own client records.
VERSION	1.0 · effective 9 November 2026 · next review 9 November 2027
POLICY OWNER	ICPHAA Board of Directors
CONTACT	ICPHAA Registry · admin@icphaa.ie

AT A GLANCE

- ICPHAA is the data controller for member, applicant and complaints records; members are controllers for their own client records.
- Personal data is processed only for defined purposes, on a lawful basis, and limited to what is necessary.
- Records are kept only as long as needed under a retention schedule, then securely destroyed.
- Qualifying personal data breaches are notified to the Data Protection Commission within 72 hours (GDPR Art. 33).
- Data protection queries and rights requests go to the ICPHAA Registry at admin@icphaa.ie.

CONTENTS

1 Purpose and scope 2
2 Roles and definitions 3
3 Data protection principles 3
4 What ICPHAA processes and why 4
5 Processors, sharing and international transfers 4
6 Retention and secure disposal 5
7 Security and personal data breaches 5
8 Data subject rights 6
9 Members as data controllers 6
10 Responsibilities, concerns and review 7

1. Purpose and scope

The Irish Counselling, Psychotherapy & Allied Healthcare Professionals Association (ICPHAA) holds personal data about members, applicants, people who raise concerns, members who are the subject of concerns, event participants and others. Members of the Association, in turn, hold some of the most sensitive personal data there is: information about their clients' health, relationships and lives. Handling that information with care is a legal obligation and an expression of respect for the people it describes.

This policy sets out how ICPHAA complies with the General Data Protection Regulation (GDPR) and the Data Protection Acts 1988–2018 in its own processing, and the standards ICPHAA expects of members as data controllers for their client records. It applies to everyone who processes personal data on the Association's behalf, including the Board, the Registry, the Accreditation Department, staff, volunteers and processors, and to every member in respect of their own practice. How the ICPHAA website handles information submitted through its forms is explained in the Privacy Policy — Website Forms.

2. Roles and definitions

TERM	MEANING IN THIS POLICY
Personal data	Any information relating to an identified or identifiable living person.
Special category data	Data revealing health, racial or ethnic origin, religious beliefs, sexual orientation and other categories listed in Article 9 GDPR. Most clinical information is health data.
Controller	The person or body that decides why and how personal data is processed. **ICPHAA is the controller** for membership, accreditation, complaints, events and governance records. **Members in independent practice are the controllers** for their own client records.
Processor	A person or body that processes personal data on a controller's behalf and on its instructions, such as an IT, email, payment or cloud storage provider.
Data subject	The living person the data is about.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

ICPHAA does not hold members' client records and does not act as controller for them. Within ICPHAA, data protection matters are handled by the ICPHAA Registry (data protection queries: admin@icphaa.ie), under the oversight of the Board of Directors.

3. Data protection principles

ICPHAA processes personal data in line with the principles in Article 5 GDPR. Personal data is:

1. processed **lawfully, fairly and transparently**, with clear privacy information given to the people concerned;
2. collected for **specified, explicit and legitimate purposes** and not used in ways incompatible with them;
3. **adequate, relevant and limited** to what is necessary for those purposes (data minimisation);
4. **accurate** and, where necessary, kept up to date;
5. **kept no longer than necessary**, in line with the retention schedule;
6. processed **securely**, with appropriate technical and organisational measures.

ICPHAA is responsible for, and must be able to demonstrate, compliance with these principles (accountability). It keeps a record of its processing activities, builds data protection into new systems and processes from the start, and carries out a data protection impact assessment before any processing likely to result in a high risk to individuals.

4. What ICPHAA processes and why

ICPHAA processes personal data only for defined purposes, each with a lawful basis under Article 6 GDPR and, for special category data, a condition under Article 9.

PURPOSE	TYPICAL DATA	LAWFUL BASIS
Membership administration and renewal	Name, contact details, category, qualifications, insurance, declarations, payment records	Contract (membership agreement); legal obligation for financial records
Accreditation and category changes	Training, practice and supervision evidence, CPD records, references	Contract; legitimate interests in maintaining professional standards
Public verification of member status	Name, category, status, membership number	Legitimate interests in public protection, explained to members at joining
Complaints, fitness to practise and discipline	Allegations, evidence, correspondence, decisions; may include health data	Legitimate interests in public protection; for special category data, the establishment, exercise or defence of legal claims or another applicable Article 9 condition
Events and CPD	Registration, attendance, access requirements	Contract; consent for optional information
Newsletters and non-essential communications	Name, email, preferences	Consent or, for members, legitimate interests with an easy opt-out

Information about criminal convictions or vetting outcomes is processed only where the law permits, including under the National Vetting Bureau (Children and Vulnerable Persons) Acts 2012–2016, and with additional safeguards.

5. Processors, sharing and international transfers

- **Processors.** ICPHAA uses processors only under a written contract meeting Article 28 GDPR, after checking that they provide sufficient guarantees of security and confidentiality.
- **Sharing.** ICPHAA shares personal data with third parties only where there is a lawful basis, for example where required by law, where needed to protect a person from serious harm, or with a public body such as Tusla, An Garda Síochána or CORU where the law requires or permits it. Any sharing is limited to what is necessary and is recorded.

- **No sale of data.** ICPHAA never sells personal data or makes it available for third-party marketing.
- **Transfers outside the European Economic Area.** Where a processor stores or accesses data outside the EEA, ICPHAA makes sure an appropriate safeguard recognised by the GDPR is in place.

6. Retention and secure disposal

ICPHAA keeps a retention schedule setting out how long each category of record is kept and why. Periods are based on the purpose of the record, legal requirements and the Association's legitimate need to deal with any later concern or claim.

RECORD	BASIS FOR RETENTION PERIOD
Membership and accreditation records	Duration of membership, then a defined period to allow verification of past status and to deal with later queries
Complaints, fitness to practise and disciplinary records	A defined period after the final decision, reflecting the need for public protection and the possibility of further proceedings
Financial records	The periods required by tax and company law
Event and CPD attendance records	As long as needed to confirm attendance and issue certificates
Marketing preferences	Until consent is withdrawn or the person unsubscribes

When a record reaches the end of its retention period it is securely destroyed: paper by confidential shredding and electronic records by secure deletion. The Registry keeps a log of disposals so that ICPHAA can demonstrate compliance.

7. Security and personal data breaches

ICPHAA protects personal data with measures appropriate to the risk, including role-based access controls, strong passwords and multi-factor authentication, encryption of sensitive data in transit and at rest where possible, secure storage of any paper records, regular review of security measures and data protection training for anyone handling personal data.

If a personal data breach occurs or is suspected:

1. The person who discovers it reports it immediately to the ICPHAA Registry at admin@icphaa.ie.
2. The Registry takes immediate steps to contain the breach and recover the data where possible.
3. The Registry assesses the likely risk to the rights and freedoms of the people affected.
4. Unless the breach is unlikely to result in a risk to individuals, ICPHAA notifies the Data Protection Commission without undue delay and, where feasible, within 72 hours of becoming aware of it, as Article 33 GDPR requires.
5. Where the breach is likely to result in a high risk to individuals, ICPHAA informs them without undue delay, in clear language, with advice on protecting themselves (Article 34 GDPR).

6. Every breach, whether notified or not, is recorded with its facts, effects and the action taken, and reported to the Board, which makes sure lessons are learned.

8. Data subject rights

ICPHAA respects and facilitates the rights of data subjects under the GDPR: the right to be informed; the right of access; the right to rectification; the right to erasure; the right to restriction of processing; the right to data portability; the right to object; and rights in relation to automated decision-making. ICPHAA does not make decisions about individuals based solely on automated processing.

Requests should be sent to the ICPHAA Registry at admin@icphaa.ie. ICPHAA will verify the requester's identity, respond without undue delay and within one month, and explain if the period needs to be extended because a request is complex. Some rights are subject to legal limits, for example where releasing information would reveal personal data about someone else or prejudice an ongoing investigation; any such limit will be explained. Anyone dissatisfied with ICPHAA's response may complain to the Data Protection Commission (www.dataprotection.ie).

9. Members as data controllers

Members in independent practice are controllers for their client records and are personally responsible for complying with data protection law. Members employed by an organisation normally process records on their employer's behalf and must follow its policies. ICPHAA expects every member to:

- identify a lawful basis and an Article 9 condition for processing client health data, and record it;
- give clients clear privacy information at the outset, alongside the explanation of confidentiality and its limits;
- collect only the information needed for safe and effective work, and keep records accurate, factual and respectful;
- store records securely, using encryption for electronic records and portable devices and locked storage for paper;
- use only secure, appropriate platforms for online work, and put a written agreement in place with any processor;
- keep client records for at least seven years after therapy ends and, for clients who were under 18, until the client reaches 25 or for seven years after therapy ends, whichever is later, then destroy them securely;
- respond to client requests to exercise their rights, including access requests, within the legal time limit;
- notify the Data Protection Commission of a qualifying personal data breach within 72 hours, and inform affected clients where the risk to them is high;
- make arrangements, through a professional will or similar, for the safe handling of client records if they become unable to practise.

10. Responsibilities, concerns and review

The ICPHAA Board of Directors owns this policy and has overall responsibility for the Association's data protection compliance. The Registry handles day-to-day data protection matters, maintains the record of processing, the retention schedule and the breach log, and is the contact point for queries and rights requests. Everyone who handles personal data on ICPHAA's behalf must follow this policy and complete the training provided.

A failure by a member to protect client data may breach the ICPHAA Code of Conduct for Members and be considered under the Complaints Procedures or Disciplinary Procedures. Concerns about ICPHAA's own handling of personal data should be sent to admin@icphaa.ie. ICPHAA cooperates fully with the Data Protection Commission in the exercise of its functions.

This policy is reviewed by the date shown on the cover, and earlier where data protection law, guidance from the Data Protection Commission or the Association's processing changes.

READ ALONGSIDE

- Privacy Policy — Website Forms
- Confidentiality Policy
- Digital & Practice Environment Policy
- Irish Regulatory Policy
- Records of Decision Policy
- Public-Facing Transparency Policy

DOCUMENT CONTROL

VERSION	DATE	CHANGE	APPROVED BY
1.0	9 November 2026	Reissued in the ICPHAA policy framework (replaces the former ICPA version).	ICPHAA Board of Directors

Support · Develop · Empower