Law Society of Ireland

GDPR GUIDE FOR SMALL LAW FIRMS

Law Society of Ireland, Blackhall Place, Dublin 7

Tel: +353 1 881 5768 | Email: solicitorservices@lawsociety.ie | www.lawsociety.ie

Contents

GDPR GUIDE
FOR SMALL
LAW FIRMS

1. Introduction and scope

The General Data Protection Regulation (EU) 2016/679 ("GDPR") has applied directly in Ireland and across the EU since 25 May 2018. The GDPR and the Data Protection Act 2018 together provide the legislative framework for data protection in Ireland. The Data Protection Commission (DPC) is the main regulator responsible for ensuring compliance with both.

This guide is intended for solicitors and practice managers in small Irish law firms who want a clear, practical understanding of what GDPR requires of them in their day-to-day operations. While some GDPR obligations scale with the size and nature of a firm's data processing activities, the core principles apply to every practice — no matter how small.

Law firms occupy a particularly sensitive position under data protection law. They routinely handle highly confidential Personal Data, sometimes including Special Category Data, particularly in the context of client representation, employment matters, litigation, conveyancing, and probate. GDPR compliance is not just a legal obligation but a core professional responsibility.

NOTE: This guide covers the most important GDPR obligations for a small Irish law firm. It does not constitute legal advice. Firms with complex processing activities or uncertainty about specific issues should seek tailored data protection advice.

KEY DEFINITIONS

- A **Data Controller** decides the purposes and means of processing Personal Data. A law firm is usually the Data Controller for the Personal Data of clients, staff, counterparties, witnesses, and others whose data you hold.
- A **Data Processor** processes data on behalf of a Data Controller, for example your practice management software provider, a cloud storage provider, or an external payroll company. You remain responsible for ensuring Data Processors are compliant.
- **Personal data** means any information relating to an identified or identifiable natural person. In a legal context, this is extremely broad and includes names, addresses, PPS numbers, financial information, details of legal matters, and correspondence.
- **Special Category Data** is a defined in Article 9 as 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 person, data concerning health or data concerning sex life or sexual orientation. Law firms may frequently handle this type of data, particularly in family law, employment, personal injury, and asylum matters. Special rules apply to the processing of this data.

2. Executive Summary – Key Points to Consider

This guide covers the most important GDPR obligations for small Irish law firms. When considering what steps your firm needs to take, it can be a useful starting point to refer to the Self-Assessment Checklist provided by the Data Protection Commission (DPC) on their web site

https://www.dataprotection.ie/sites/default/files/uploads/2022-01/Self-assessment%20checklist.pdf

In particular, there are certain key points for your firm to consider: -

1) **Privacy Notice.** If you don't already have one on your web site, refer to the template provided by the Law Society and tailor it as needs be to your firm. If you have one, review it against this template to ensure its fit for purpose. **www.lawsociety.ie/essentials-in-practice-toolkit/**

2) **Data Protection Policy for Staff.** Again, if you don't already have one, refer to the template provided by the Law Society and tailor it as needs be to your firm. If you have one, review it against this template to ensure its fit for purpose. **www.lawsociety.ie/essentials-in-practice-toolkit/**

3) **Security.** The #1 Data Protection risk for all organizations regardless of size is the security of personal data held. As a priority, refer to the section on Security in this Guide and consider whether your firm has sufficient measures in place.

4) **Training.** The most common cause of all data security breaches in organizations (reported to the DPC) is human error. Ensure your firm provides mandatory Data Protection training to all your staff and keep a record of all such training.

5) **Data Protection Officer (DPO)/Data Protection lead.** Consider whether your firm is required to have a DPO. If your firm has one, make sure their contact details are notified to the DPC. In any event, all organizations should have a designated Data Protection lead to co-ordinate all Data Protection matters and to act as contact point both internally and externally.

6) **Records.** Make sure your firm has a Retention policy/schedule and that you implement it in practice by operating a data deletion/shredding cycle at least annually. Consider also whether your firm is required to have Record of Processing Activities (RoPA) in place. For ease of use, these two records can be combined.

7) **Data Protection Impact Assessments (DPIAs).** Consider whether your firm needs to carry out a DPIA.

3. Understanding the legal framework

The GDPR is built on a set of core data protection principles set out in Article 5. Every time your firm processes Personal Data, you must comply with all of them.

Core data protection principles as set out in Article 5 GDPR

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

1.Lawfulness, fairness and transparency

You must have a valid legal basis for processing Personal Data; processing must not be misleading or harmful, and people must be told how their data will be used. For a law firm, this means that e.g. when you take on a new client, you need to have identified your legal basis for processing their data, and your client care letter or privacy notice must explain clearly how that data will be used.

2.Purpose limitation

Data collected for one purpose must not be used for a different, incompatible purpose without further justification. If you collect a client's contact details and financial information to act for them in a conveyancing transaction, you cannot then use that information in an incompatible way, without a separate basis for doing so. A good rule of thumb is to consider whether the person would expect their data to be used in this way. If not, consider whether you have a valid legal basis for the processing and update your privacy notice.

3.Data minimisation

You should only collect and retain data that is adequate, relevant and limited to what is necessary for the purpose. A firm acting in a straightforward conveyancing claim does not need to collect the client's extensive background medical history. Similarly, asking clients to provide more identity documentation than AML requirements strictly demand would breach this principle.

4.Accuracy

Personal Data must be kept accurate and up to date, and inaccurate data should be corrected or deleted promptly. This has particular importance in litigation, where errors in a party's address or identity details can have procedural consequences. It also matters in ongoing client relationships, where out-of-date contact details may mean correspondence does not reach the right person.

5.Storage limitation

Data must not be kept for longer than is necessary. Your firm needs to have a documented Retention policy/schedule setting out (i) the categories of data held; (ii) the reason for the retention: either a particular legal/regulatory requirement (e.g. AML) or a business need; and (iii) the particular retention period. Retaining client files indefinitely because it is easier than reviewing them will breach this principle.

6.Integrity and confidentiality.

Data must be protected against unauthorised access, accidental loss, or destruction, using appropriate technical and organisational security measures. Sending an email containing a client's medical report to the wrong recipient, failing to password-protect documents sent externally, and storing paper files in an unsecured area accessible to non-staff are all examples of failures under this principle.

7. Underpinning all of these is the principle of **accountability** (Article 5(2)): the firm, as Data Controller, must not only comply with the GDPR but must be able to demonstrate that it does so. This means having documented policies and staff training records.

4. Lawful basis for processing

Under Article 6 GDPR, you must identify a specific lawful basis before you process any Personal Data. The most relevant basis for a small law firm are as follows.

Contract (Article 6(1)(b)). Processing is necessary to perform a contract with the Data Subject, or to take steps at their request before entering into a contract. For a law firm, this is the appropriate basis for processing the Personal Data of individual clients as it is genuinely necessary to deliver the legal services, they have engaged you to provide. For example, using a personal injury client's name, address, PPS number, employment details and medical history to pursue their claim is processing necessary to perform the retainer. Using their contact details to send them matter updates is similarly covered. The important qualifier is necessity: if the data is not actually required to carry out the work, contract is not the right basis.

Legal obligation (Article 6(1)(c)). Processing is necessary to comply with a legal obligation. This is the basis for data you are required to hold under anti-money laundering legislation, including client identity and verification records. It also covers returns to the Revenue Commissioners and responses to court orders requiring disclosure of information.

Legitimate interests (Article 6(1)(f)). Processing is necessary for the purposes of the legitimate interests of the Data Controller or a third party, except where those interests are overridden by the interests or rights of the Data Subject. This basis requires your firm to undertake and document a three-part test.

1. identify the legitimate interest,
2. show that the processing is necessary for that interest
3. balance it against the Data Subject's interests

Example: CCTV

A law firm may rely on legitimate interests for activities such as using CCTV.

In this case, the three-part test might be met as follows

- Legitimate interest identified
  - Securing your firm's property and premises.
- Processing is necessary for that interest
  - CCTV is an essential tool in deterring and prosecuting crime and is an insurance requirement.
- Balance it against the Data Subject's interests
  - Your firm's CCTV is clearly visible with signage stating its purpose.

A good rule of thumb is whether an individual (visitor, client, passer-by) would reasonably expect your firm to have CCTV.

Important: It's important to document this three-part test because this particular legal basis is open to challenge by a Data Subject (see Right to Object in section 4 below).

This legal basis is not available where the processing involves Special Category Data (e.g. health data).

Consent (Article 6(1)(a)). The Data Subject has given clear, specific, informed and unambiguous consent. Consent must be freely given, which means it cannot be a condition of receiving legal services. It must be as easy to withdraw consent as it is to give consent. For most routine client data processing, consent is not the right basis. However, it may be appropriate where you wish to send a client marketing communications about your firm's events and publications or use their Personal Data in a testimonial. In those cases, a clear opt-in mechanism is required (consent cannot be presumed), and you must be prepared to honour withdrawal of consent promptly. Records must be kept and maintained, and best practice would usually involve an automated solution linking a client's consent preference to their client profile.

Important: You must identify your lawful basis before you begin processing, not retrospectively.

LAWFUL BASES FOR SPECIAL CATEGORY DATA

If you are processing Special Category Data, you need both a lawful basis under Article 6 and a separate condition under Article 9(2). The most relevant conditions for a law firm are as follows.

Article 9(2)(f). Processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity. This is the principal basis for a law firm processing Special Category Data. A personal injury or medical negligence file will typically contain extensive medical records, and a family law file may contain health information about the parties. Provided the processing is necessary for the legal claim or proceedings, Article 9(2)(f) provides the condition required.

Article 9(2)(b). Processing is necessary for carrying out obligations in the field of employment, social security and social protection law. This is relevant for firms advising on employment law matters where processing of data about trade union membership, health or protected disclosures may be necessary.

Article 9(2)(a). Explicit consent from the Data Subject. This requires a clear, affirmative statement from the individual, going beyond the standard consent requirements of Article 6. The same caveats about freely given consent apply; it cannot be bundled into general terms of engagement and must be specific to the processing in question.

The DPC's guidance on legal bases for processing personal data can be found here.

https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Legal%20Bases.pdf

5. Data subject rights

The GDPR gives individuals a range of rights in relation to their Personal Data. As a Data Controller, your firm must be prepared to respond to requests exercising these rights within statutory time limits as set out below.

Right of access (Article 15), the Data Subject Access Request or DSAR. Individuals can request a copy of all Personal Data you hold relating to them, along with supplementary information about how it is used. The response must be provided to the data subject within one calendar month and is generally free of charge (so you cannot charge the data subject for the work involved). The time limit can be extended by two further months for complex or voluminous requests, but you must notify the requester of the extension and the reasons for the extension within the first month (and ideally as soon as possible). In a law firm context, DSARs most commonly arise from former clients, employees (current and former), or counterparties. A former client requesting all data held relating to them, or an employee involved in a disciplinary process seeking the contents of their personnel file, are typical examples. Refer to the Law Society's Guidance on Data Subject Access Requests (DSARs) Handling in Law Firms for further information. **www.lawsociety.ie/essentials-in-practice-toolkit/**

The DPC's FAQs and guidance on DSARs can be found here:

https://www.dataprotection.ie/sites/default/files/uploads/2019-10/FAQ%20Guide%20to%20Data%20Subject%20Access%20Requests_Oct19.pdf

https://www.dataprotection.ie/sites/default/files/uploads/2025-05/20221005_Subject_Access_Requests_A_Data_Controller's_Guide.pdf

Right to rectification (Article 16). Individuals can require you to correct inaccurate Personal Data that you hold relating to them, and to complete incomplete Personal Data. You must respond within one calendar month, with the possibility of a two-month extension for complex requests, provided you notify the individual within the first month and explain the reason for the delay.

The right has two distinct limbs. The first concerns accuracy: where data is factually wrong, the individual can require correction. For example, if a client's name has been recorded incorrectly on your system, or an employee's address is out of date, they are entitled to have this corrected. The second concerns completeness: where data is incomplete, they can require that it be completed, including by means of a supplementary statement. An employee whose file records only part of training they undertook, might invoke the second.

The right applies only to inaccurate or incomplete data. Where you hold a record of something that the Data Subject disputes but which is, in fact, accurate, the right to rectification does not require you to alter it. A key example in the law firm context is file notes and attendance notes. If a file note records what was said in a meeting, and the client later disputes the content of that note, the client does not have an automatic right to have the note changed simply because they disagree with what it says. An appropriate response may be to note on the file that the client disputes the content, without altering the original record.

Right to erasure, also known as the Right to be Forgotten (Article 17). Individuals can ask you to delete their Personal Data in certain circumstances, i.e. where it is no longer necessary for the purpose for which it was collected; where you are relying on consent as your legal basis and it is withdrawn; where the Data Subject objects to the processing and there is no overriding

legitimate grounds for processing; if the data is being unlawfully processed; or where the Personal Data is required by Irish/EU law to be erased. This right is not absolute. It does not override a firm's legitimate need to retain data for ongoing or completed legal matters, your obligations under AML legislation to retain client identity records for a prescribed period, or the applicable limitation periods to retain certain records.

Right to restriction of processing (Article 18). Individuals can ask you to restrict the processing of their Personal Data in certain defined circumstances. Restriction means that the data may be stored but not otherwise used.

The right to restriction arises in four situations. First, where the individual contests the accuracy of the data, restriction applies while accuracy is being verified. Second, where the processing is unlawful, but the individual prefers restriction to erasure, they can require that you retain the data but cease processing it. Third, where you no longer need the data for the purposes for which it was collected but the individual needs it retained for the establishment, exercise or defence of legal claims. Fourth, where the individual has objected to processing under Article 21 and a decision is pending as to whether your legitimate grounds override theirs.

The second of these circumstances deserves particular attention in a law firm context. Where a firm has been processing Personal Data without a valid lawful basis, the individual is not required to choose between leaving the data in active use or demanding its deletion. They have a third option: to require that the data be retained but quarantined from further processing until the underlying issue is resolved.

A practical example would be where a firm has been using a former client's contact details to send them marketing communications without obtaining the necessary consent and without another valid basis for doing so. The former client objects and raises a complaint. Rather than requesting deletion of their contact details, the individual may prefer to invoke the right to restriction. This might be because they anticipate needing to reference that correspondence in a complaint to the DPC or in other proceedings and wish to ensure the data is preserved rather than destroyed. The effect of the restriction is that the firm must retain the data but must cease all processing of it other than storage, including ceasing the marketing communications that gave rise to the complaint in the first place. The firm cannot use, share, or act on the restricted data without the individual's consent, except for the purpose of storage or in connection with legal claims.

When processing is restricted, you must inform the individual before lifting the restriction. If the restricted data has been shared with third parties, you should inform them of the restriction where possible, unless this is impossible or involves disproportionate effort.

Right to data portability (Article 20). This applies where processing is based on consent or contract, is carried out by automated means and only applies to Personal Data that the individual has provided to the Data Controller. Individuals can ask for their data in a structured, commonly used, machine-readable format. This is relatively limited in relevance for typical law firm processing.

Right to object (Article 21). Where processing is based on legitimate interests, individuals have a right to object to the processing, though this can be overridden where the Data Controller demonstrates compelling legitimate grounds. The individual must provide grounds relating to their particular situation, and the law firm can override the objection if it can demonstrate compelling legitimate grounds for the processing that override the interests, rights and freedoms of the individual, or if the processing is necessary for the establishment, exercise or defence of legal claims.

Individuals also have an absolute right to object to their data being used for direct marketing purposes, e.g. if a former client asks to be removed from your mailing list, you must act on that request without exception.

PRACTICAL STEPS FOR RIGHTS MANAGEMENT

Your firm should designate an individual responsible for handling Data Subject requests. You should have an internal process for identifying, locating and retrieving relevant data across all systems, including case management software, email archives, paper files and any cloud storage. Remember, not all Personal Data held relating to an individual is disclosable in response to a DSAR, restrictions may apply, for example, privilege over communications prepared for the dominant purpose of litigation. You should seek specialist advice on borderline cases rather than assuming all data can be withheld or that all data must be disclosed.

6. Records of Processing Activities (RoPAs)

Under Article 30 GDPR, organisations with 250 or more employees are required to maintain a formal Record of Processing Activities. Organisations below this threshold must still maintain records where they carry out processing regularly that involves Special Category Data/criminal convictions/offences data, or processing that could result in a risk to the rights and freedoms of Data Subjects. In practice, this means that law firms specialising in personal injury, criminal matters or that process large volumes of Special Category Data will have to create and maintain a RoPA.

Even where there is technical doubt about whether the obligation applies, maintaining a RoPA is fundamental to accountability and is recommended as a matter of good practice. It is also essential for demonstrating compliance to the DPC in the event of an investigation or complaint.

Your RoPA should contain the following, as required by Article 30:

- The name and contact details of your firm as Data Controller, and of your DPO/data protection contact person.
- The purposes of each processing activity. For a small law firm, typical entries would include client matter management, anti-money laundering compliance, HR and payroll, marketing communications, and accounts and billing.
- The categories of Data Subjects, for example clients, counterparties, witnesses, employees, job applicants.
- The categories of Personal Data processed. A client matter entry might include identity data, contact data, financial data, and, where relevant, health data or other Special Category Data.
- The categories of recipients, for example, courts, counsel, expert witnesses, banks, the Revenue Commissioners, the LSRA, the Law Society and IT or cloud service providers that act as Data Processors.
- Details of any transfers to third countries and the safeguards in place. If your practice management system is hosted by a US provider, this needs to be recorded.
- Retention periods, how long each category of data is held, by reference to your retention schedule.

Your RoPA does not need to be a complex document. A well-maintained spreadsheet or table is perfectly adequate. It should be reviewed and updated at least annually, and whenever you introduce a new processing activity, new software, or a new type of client work.

For DPC examples of best practice RoPAs, refer to the DPC guidance at **https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Records%20of%20Processing%20Activities%20%28RoPA%29%20under%20Article%2030%20GDPR.pdf**

7. Privacy notices and transparency

Articles 13 and 14 of the GDPR require you to provide individuals with specific information about how their Personal Data will be used, at the time it is collected. This is usually achieved by drafting a privacy notice and making it available on your website/ at your reception desk etc.

A privacy notice must contain, at minimum: the identity and contact details of the Data Controller; the purposes and lawful bases for processing; the legitimate interests relied upon where applicable; the recipients or categories of recipients; details of any international transfers and the safeguards in place; retention periods; the individual's rights and how to exercise them; the right to lodge a complaint with the DPC; and whether providing Personal Data is a statutory or contractual requirement.

For a law firm, the primary vehicles for client-facing transparency are the client care letter or retainer agreement, which should reference your privacy notice, and a standalone privacy notice published on your website or provided in hard copy at the point of engagement.

For employees, a separate staff privacy notice is required (usually referred to as a data protection policy for staff), covering HR-specific processing such as payroll, performance management, disciplinary processes and any monitoring activities. If your firm uses any form of access logging, call recording, or email monitoring, those activities must be disclosed in the staff privacy notice.

Please refer to the Law Society templates for Privacy Notices (for clients and third parties etc) and Data Protection Policy (for staff). **www.lawsociety.ie/essentials-in-practice-toolkit/**

8. Data security and breach management

SECURITY OBLIGATIONS

Article 32 requires you to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Appropriateness is assessed having regard to the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the likelihood and severity of risks to individuals.

For a law firm, the baseline security measures expected include the following:

- Implement strong password policies and multi-factor authentication for all systems containing client data, including email, case management software and cloud storage.
- Implement controls/alerts for the downloading of large volumes of data.
- Laptops and portable devices should be encrypted.
- Documents containing Personal Data should be transmitted by secure means where possible, and staff should be trained not to send unprotected sensitive documents by unencrypted email.
- Regularly apply security updates and patches to all systems.
- Store physical files in locked cabinets, with controlled access to sensitive case material.
- Regular staff training on phishing and social engineering is essential, since the majority of breaches in professional services firms involve human error rather than technical vulnerabilities.
- Documented access controls should limit data access to those who need it, so that, for example, a fee earner working on a commercial law matter cannot routinely access files from the family law department.
- Conduct regular secure backups with tested restoration procedures ensure that a ransomware attack or system failure does not result in permanent data loss.
- Periodically review security measures and conduct internal audits to identify vulnerabilities.

Organisational measures matter as much as technical ones. Some examples for a small law firm are:

- Clear desk policy
- Secure document disposal procedure using cross-cut shredding or a confidential waste contractor
- Policy on the use of personal devices for work purposes.
- Educate all staff - partners, solicitors, administrative staff, trainees etc on their GDPR responsibilities. Include practical training on:

- Identifying phishing emails
- Secure file handling
- Data breach processes
- Managing client data securely
- Data subject rights

The DPC's guidance on Data Security can be referred to here. https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Data_Security_Guidance_Feb20.pdf

PERSONAL DATA BREACHES

A Personal Data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. In a law firm context, common examples include sending a document containing confidential client information to the wrong email address, losing an unencrypted laptop or USB drive, a ransomware attack encrypting the firm's systems, or discovering that a former member of staff retained access to the case management system after leaving. All of these are breaches that require assessment and potential reporting.

Under Article 33, if a breach is likely to result in a risk to the rights and freedoms of individuals, **you must notify the DPC without undue delay and in any event within 72 hours of becoming aware of it.** Where notification is delayed beyond 72 hours, you must provide reasons for the delay. The threshold for notification is not a high one: if there is any meaningful risk to individuals, reporting is required. The DPC expects organisations to notify a data breach via a portal which can be accessed here.

https://forms.dataprotection.ie/breach-notification

Under Article 34, if the breach is likely to result in a high risk to individuals, you must also notify the affected individuals directly without undue delay. A breach involving health data, financial data, or data about vulnerable individuals will generally require individual notification.

All breaches must be logged internally under Article 33(5), even those that do not need to be reported to the DPC. Your breach log should record the facts, the effects, and the remedial action taken. Maintaining this log is important both for accountability purposes and because the DPC may ask to see it during any investigation.

> **Important:** The 72-hour notification window begins when any person in the organisation becomes aware of the breach, not when the partner reviews it. You should have an internal escalation procedure so that all staff know to report suspected breaches immediately to the designated person, who can then carry out a risk assessment to determine risk level and whether notification is required.

Even with strong safeguards, data breaches can still occur. Having a clear, documented plan reduces risk and ensures regulatory compliance.

Your breach response plan should include:

- How staff should identify potential breaches and how and to whom should they escalate the issue.
- How the DPO/ designated contact person should assess the severity and impact of a breach.
- How the DPO/ designated contact person should determine whether a report to the Data Protection Commission is required within the 72-hour deadline.
- How the DPO/ designated contact person should notify affected individuals if necessary.
- How to document the incident, actions taken and lessons learned.

Conducting practice exercise or tabletop scenarios can help staff prepare.

The DPC's guidance on data breach notifications can be referred to here. https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf

The Law Society's Data Breach Protocol can be found here. https://www.lawsociety.ie/intellectual-property--data-protection-law

9. Third parties and Data Processors

Whenever you engage a third party to process Personal Data on your behalf, Article 28 GDPR requires you to have a written Data Processing Agreement (DPA) in place. Data Processors include entities that store the data on your behalf.

For a small law firm, the most common data processors in a law firm context include:

- Cloud-based practice management systems (e.g. SharePoint)
- Document management platforms
- Case management platforms (for timekeeping)
- e-discovery or document review services
- Dictation software providers
- IT support and managed services providers
- External HR and payroll providers
- Archive and shredding providers
- Stenographers
- any other vendor who has access to Personal Data held by the firm.

The requirement is not limited to large or complex providers: if your bookkeeper processes payroll data on your behalf, a DPA is required.

The DPA must include mandatory clauses covering the following:

- the subject matter, duration, nature, and purpose of the processing
- the types of Personal Data and categories of Data Subjects involved
- the obligations and rights of the Data Controller (i.e. your firm)
- the Data Processor's obligation to act only on your firm's documented instructions (including regarding transfers of Personal Data to non-EEA countries)
- confidentiality obligations
- security requirements
- conditions for engaging sub-processors
- obligations to assist with Data Subject rights and breach notifications
- deletion or return of data on termination of the provision of services
- audit rights

Many vendors provide standard DPAs as part of their terms of service, but you should review these rather than assuming they are adequate.

Every law firm should maintain a register of your Data Processors. Before engaging any new vendor with access to Personal Data, you should carry out due diligence on their data protection and security arrangements and review their data processing clauses/ DPA. Asking a prospective IT provider whether they are ISO 27001 certified (specifically ISO/IEC 27001:2022), where they host data, and whether they have experienced any breaches in the past two years is a reasonable starting point.

Where you share Personal Data with another party acting as a separate Data Controller, for example instructing counsel or referring a client to a specialist firm, you are not engaging a Data Processor but rather disclosing data to another Data Controller. You must ensure you have a lawful basis for that disclosure, and your privacy notice should inform clients of those categories of recipients.

The DPC's guidance on Controller-Processor Contracts can be referred to here.

https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190624%20Practical%20Guide%20to%20Controller-Processor%20Contracts.pdf

10. Special Category Data

Given the range of legal work carried out by most law firms, the handling of Special Category Data deserves specific attention.

Article 9 of the GDPR lists the "special categories of personal data" as: -

1. Personal data revealing racial or ethnic origin;
2. Political opinions;
3. Religious or philosophical beliefs;
4. Trade union membership;
5. Genetic data and biometric data processed for the purpose of uniquely identifying a natural person;
6. Data concerning health;
7. Data concerning a natural person's sex life or sexual orientation.

Health data arises constantly: personal injury and medical negligence files routinely contain GP records, hospital reports, specialist opinions, and prognosis reports. Employment files may contain details of disability, mental health conditions or absences attributed to illness. Family law files frequently contain health information about parties or children. Each of these requires both a lawful basis under Article 6 and a condition under Article 9(2), as described in Section 3. Data revealing racial or ethnic origin and religious beliefs frequently appears in family and immigration files and may also arise in employment discrimination cases. Data about trade union membership is relevant in industrial relations matters.

Criminal conviction and offence data, which is governed by Article 10 rather than Article 9 but attracts similar heightened protection, arises in criminal defence work and in certain regulatory or disciplinary proceedings.

In each case, you must be able to identify and document both the Article 6 legal basis and the applicable Article 9 or Article 10 condition. You should apply heightened security to files and electronic records containing Special Category Data, including access restrictions so that the file can only be opened by those working on the matter, encryption of any documents transmitted externally, and explicit records of who has accessed the file. Special Category Data should feature prominently in your RoPA, with the relevant conditions identified for each processing activity.

11. Data Protection Officer

Article 37 GDPR requires certain organisations to designate a Data Protection Officer (DPO). The obligation applies where the core activities of the organisation consist of processing operations which, by virtue of their nature, scope and purposes, require regular and systematic monitoring of Data Subjects on a large scale, or where the Data Controller processes Special Category Data or criminal offence data on a large scale.

For most small law firms, the mandatory DPO obligation may not arise. A general practice firm with a small number of fee earners processing client data in the ordinary course of legal work is not processing on a scale that triggers the obligation. It is however good practice for law firms to designate an internal data protection lead/contact point who takes responsibility for co-ordinating Data Protection training, policies, access requests, and breach management, even if that person is not formally titled DPO. In a small firm, this role often falls to a senior partner or the practice manager.

Important: Even if your firm is small in size with a small number of fee earners but handles significant personal injury or clinical negligence work at large scale, you will need to assess whether the mandatory obligation applies. A firm that processes medical records for a large panel of insurance clients, or that operates a significant outsourced document review function, may well cross the threshold. Should your firm have a DPO or decide to appoint one, the DPO's contact details must be notified to the DPC.

To assess whether your firm is required to appoint a DPO, you should refer to the DPC's guidance here.

http://www.dataprotection.ie/en/dpos/who-needs-dpo

12. Data transfers outside the EEA

Chapter V of the GDPR restricts the transfer of Personal Data to countries outside the European Economic Area (EEA) unless an appropriate safeguard is in place. Some examples of where this may arise in practice are:

- Using cloud software hosted on servers outside the EEA: if your practice management system, email platform, or document storage is provided by a US company and data is stored on US servers, that is a transfer to a third country requiring a lawful mechanism.
- Instructing foreign counsel or experts in cross-border matters involves sharing Personal Data with recipients outside the EEA.
- Acting in international commercial or family matters may require disclosure of Personal Data to parties, courts, or authorities in non-EEA jurisdictions.

The primary mechanisms for lawful transfers are as follows:

- An adequacy decision from the European Commission which confirms that the third country provides an equivalent level of data protection, and transfers can proceed without further safeguards.
- Standard Contractual Clauses (SCCs), issued by the European Commission, are contractual provisions incorporated into agreements with the recipient that provide a legal basis for the transfer. These are commonly used where a software provider is based in a non-adequate country but is willing to execute SCCs as part of their terms.
- In limited circumstances, derogations under Article 49 are available: most relevantly for law firms, Article 49(1)(e) permits transfers necessary for the establishment, exercise or defence of legal claims, which will cover many situations where a firm is sharing data with foreign counsel or a foreign court in the context of proceedings.
- The EU-US Data Privacy Framework, adopted in 2023, is the current adequacy mechanism for transfers to US-based organisations that have certified under the Framework. If your practice management or email provider is based in the US, you should check whether they are a certified participant (by checking the List on dataprivacyframework.gov).
- Transfers to the UK are currently covered by an adequacy decision. The DPC's web site provides a list of all countries covered by an adequacy decision.

The DPC's guidance on Transfers can be referred to here. https://www.dataprotection.ie/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations

13. Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is essentially a data protection risk assessment. Article 35 of the GDPR provides that a DPIA is mandatory where a data processing activity "is likely to result in a high risk to the rights and freedoms of natural persons".

It must be carried out at the beginning of any high-risk project, for example, if the firm is adopting a new technology with access to personal data e.g. a case management or HR software system.

In cases where it is not clear whether a DPIA is mandatory, carrying out a DPIA is still good practice and a useful tool to help data controllers comply with data protection law and identify and mitigate any data protection risks in the project at the beginning.

The DPC's guidance on DPIAs (including when a DPIA is required along with a DPIA template) can be referred to here.

https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments

14. Building a culture of compliance

GDPR compliance is not a one-time project. It is an ongoing obligation that requires active management. The most common failure in small organisations is not wilful non-compliance but simply losing sight of data protection responsibilities as the firm's work expands and evolves.

Practical steps to embed a compliance culture include the following:

- Tone from the top. Ensure that your firm's partners and senior management demonstrate and communicate a real commitment to good Data Protection compliance and lead by example.
- Designate a named individual, whether a partner or the practice manager, who co-ordinates all data protection matters and acts as contact point both internally and externally.
- Incorporate data protection training into the induction of all new staff and provide annual refresher training: a new fee earner who does not understand the basics of lawful processing or the requirement to report a suspected breach promptly is a compliance risk; a staff member involved in manual activities (e.g. handling outward postal correspondence to clients and others) will need particular training on the common breaches that can occur due to human error.
- Add a data protection check to your matter-opening process, identifying what Personal Data will be collected, the lawful basis, and any special category considerations, before the first substantive step is taken in a new matter. This can trigger a RoPA and Privacy Notice update if there are new types of data being collected.
- Review your client care letter and privacy notice annually to ensure they reflect how the firm actually processes data.
- Ensure that any new software or technology is assessed for data protection compliance before it is deployed: introducing a new cloud-based dictation tool or a client portal without considering the data protection implications is a common source of compliance gaps.
- Consider data protection at the outset of any new type of work or new business process. If the firm begins offering a new service area, takes on a new category of client, or starts using a new technology tool, that is the moment to ask: what Personal Data will we be collecting, on what basis, how will we keep it secure, and how long will we keep it and do we need to carry out a DPIA?
- Carry out the DPC's Self-Assessment Checklist (refer to the Executive Summary in this Guide), identify any gaps, and create an action plan with timeframes for completion.

The Law Society of Ireland provides guidance and resources for firms on GDPR compliance and the intersection with professional obligations. The DPC's website at dataprotection.ie contains guidance on a range of processing topics including lawful bases, Data Subject rights, and data breach notification, all of which are directly relevant to legal practitioners. The DPC's guidance section is worth reviewing periodically as new materials are added.

This guide was prepared by Pembroke Privacy Limited for general information purposes. It reflects the law as of April 2026. It does not constitute legal advice and should not be relied upon as such. Firms with specific compliance questions should obtain tailored professional advice.

This resource was developed by Pembroke Privacy in consultation with the Law Society of Ireland.

Solicitor Services Department
Law Society of Ireland,
Blackhall Place, Dublin 7,
D07 VY24