Law Society of Ireland

DATA PROTECTION POLICY FOR EMPLOYEES

Law Society of Ireland, Blackhall Place, Dublin 7

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

DATA PROTECTION POLICY FOR EMPLOYEES

Data Protection Policy for Employees

Effective date: **[insert date]**

Who are we?

We are **[insert law firm name]**, your employer. Our offices are located at **[insert address]**.

[insert law firm name] is the Data Controller in respect of Personal Data which we collect and process.

Details of Personal Data processing

As a Data Controller, we collect and process “Personal Data”. Personal Data means any information relating to an individual from which that person can be identified (“Data Subject”).

During your employment with us, we collect and process your Personal Data as set out in this Data Protection Policy for Employees (“Data Protection Policy”). This includes data we receive directly from you and certain information generated in the course of your employment where it relates to you (e.g. performance reviews).

We will only process Personal Data for the purposes set out in this Data Protection Policy or for any other purposes specifically permitted by applicable law.

Scope

This Data Protection Policy applies to all who work with us, whether as employees, contractors on a temporary or permanent basis (referred to in this policy as “Staff”).

Part 1 sets out how the Personal Data that we collect relating to you is processed by us. Please read the policy carefully to understand our practices regarding your Personal Data. It also sets out your data protection rights as Staff.

Part 2 sets out your data protection obligations as Staff. It provides an overview of data protection definitions and principles. It details your obligations when dealing with Personal Data while working with us.

You agree that you will comply with the data protection obligations included at Part 2 of this Data Protection Policy, when handling Personal Data during your employment/contract with us. This includes Personal Data relating to any Staff, clients, suppliers or other people whose data we collect and process.

Any breach of these Policies may result in disciplinary action.

Any queries about this Data Protection Policy can be sent to our **[Data Protection Officer OR Data Protection contact point]** at **[insert contact point email]**

> ***For law firms to indicate which applies to your law firm: Refer to the Law Society GDPR Guide for guidance on whether your firm requires a DPO www.lawsociety.ie/intellectual-property--data-protection-law***

Information we collect about you and purposes of processing

We have set out in the table below details of the types of Personal Data, purposes and lawful basis for its processing.

Type of Personal Data	Purposes and Details of the Processing Activity	Lawful Basis for Processing
Personal Data		
• Managing and administering employment contract • Full name • Title • Phone/email address • Date of birth • PPS number • ID (passport/drivers' licence • Visa (where applicable) • Bank account details (IBAN/ BIC) • Next of kin/emergency contact details • Performance review data	Managing employment contract, performance review, pension, payroll	Contract, Legal Obligation
• Recruitment/job applications • Full name • Title • Phone/email address • CV • Completed application form (where relevant) • References	We process your Personal Data to consider your job application, to contact you about the interview process, to obtain references from third parties and to communicate the result of the job application process to you.	Consent, contract
Security • Access cards/work ID cards • CCTV	For security purposes we operate 1. Access/security protocols 2. CCTV	Contract, Legitimate Interests

[**May or may not be relevant to your firm]** Taking photographs of Staff in the workplace	We may on occasion take photographs in the workplace to display on our social media feeds and website for promotion and marketing purposes. You have the right to withdraw this consent at any time, but any processing that we have carried out before you withdrew your consent remains lawful.	Consent
[May or may not be relevant to your firm. If relevant your firm will need an Acceptable Usage Policy to cover it] Access logging, call recording, email monitoring	We may use such monitoring to ensure our firm's policies are complied with by Staff.	Contract
Special Category Data		
Only where relevant in the context of recruitment/job applicants: • Health data • Racial/ethnic origin data • Background checks / vetting which may include details of criminal convictions	We process this data where relevant for the purposes of recruitment and retain it only for so long as it is needed for that purpose.	Consent (at recruitment stage), Contract (as per your employment contract with us).
• Managing and administering employment contract • Health data	We may process this data as part of managing your employment contract including for sickness leave, occupational health and health emergency purposes.	Contract, Legal Obligation, Vital Interests

When you become our employee, the processing of your personal data will become a condition of the contract between us. If you do not provide your information when requested, we may be unable to employ you.

Who do we share your Personal Data with?

During your employment, we may be required or permitted to share your Personal Data with certain categories of third parties. Any such disclosure will be made only to the extent necessary and in accordance with our legal obligations.

The categories of third parties with whom we may share your Personal Data, and the basis on which we do so, are set out below.

- **Statutory and Regulatory Authorities**
  We may be required by law to disclose your Personal Data to statutory bodies and public authorities, including but not limited to:
  - Law enforcement agencies, where we are under a legal obligation to report, cooperate with an investigation, or comply with a court order or warrant.
  - Courts Services and the judiciary including tribunals and similar bodies, including in the context of issuing or responding to proceedings, filing documents, or complying with orders of any court or tribunal of competent jurisdiction.
  - The Revenue Commissioners, in connection with our legal obligations.
  - The Law Society of Ireland, the LSRA and the LPDT, in the exercise of its regulatory, disciplinary, or complaints-handling functions.
  - Other competent public authorities or regulatory bodies, where disclosure is required by law or necessary for compliance with a legal obligation to which we are subject.
  - Others, for example emergency services personnel (ambulance services) to protect vital interests.
- **Business Transfers**
  In the event that our firm is subject to a merger, acquisition, restructuring, sale of all or part of our practice, or similar transaction, your Personal Data may be transferred to the successor practice or acquiring entity as part of that transaction. We will take reasonable steps to ensure that any such recipient is bound by obligations of confidentiality and data protection equivalent to those that apply to us. You will be notified of any such transfer to the extent required by applicable law.

Attached below in **Schedule 1** is a list of all categories of third-party Data Processors with whom your Personal Data is shared.

Third-Party Information

During your employment, we may obtain information about you from third parties and/or you may give us information about third parties (for e.g. receiving and sharing information with the Law Society of Ireland). All such obtaining or disclosure of information is made expressly on the basis of relevant Irish or EU law which carries appropriate safeguards for you and any third-party data subject.

How long do we keep hold of your information?

We only collect the amount of Personal Data that is necessary for us to fulfil our obligations as your employer. We will only keep that data for as long as necessary.

Do we transfer your information outside the European Union or European Economic Area (EEA)?

Are any of the service providers/suppliers used by your firm to process Staff data (e.g. Payroll) located outside the EU or the EEA (Norway, Iceland Liechtenstein) OR for example does your IT Cloud provider store your Staff data in a country outside the EU/EEA?

If No, choose the following wording:

No, the recipients set out in **Schedule 1** are all located inside the EU/EEA.

If yes, choose the following wording:

The recipients set out in **Schedule 1** may be located inside or outside the EU/EEA.

- Certain recipients are in a country outside of the EU/EEA that is recognized as providing an adequate level of data protection from an EU General Data Protection Regulation perspective. These countries are: The UK, Andorra, Argentina, Brazil, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, and Uruguay. (For copies of the EU Commission adequacy decisions in relation to each of these countries, refer to commission.europa.eu)
- Certain recipients in the U.S. are certified under the EU-U.S. Data Privacy Framework and thereby also recognized as providing an adequate level of data protection from a European data protection law perspective.
- Other recipients may be in countries which do not adduce an adequate level of protection from an EU General Data Protection Regulation perspective. All necessary measures will be taken to ensure that transfers out of the EU/EEA are adequately protected as required by applicable data protection law.
- With respect to transfers to countries not providing an adequate level of data protection, we may base the transfer on appropriate safeguards, such as standard data protection clauses adopted by the European Commission (“Standard Contractual Clauses”) or by a supervisory authority, approved Binding Corporate Rules, approved code of conducts together with binding and enforceable commitments of the recipient, or approved certification mechanisms together with binding and enforceable commitments of the recipient.
- The data transfer to Data Processors which are neither certified under the EU-U.S. Data Privacy Framework nor in a country with an adequacy decision will typically also be protected by such standard data protection clauses.

Automated decision-making, profiling and artificial intelligence:
We do not use automated decision-making without human intervention, including profiling, in a way that produces legal effects concerning you or otherwise significantly affects you.

We use artificial intelligence in line with our AI Policy. For further details contact **[insert AI contact point]**.

What are your rights with respect to your Personal Data?

You have the following rights:

- The right to request a copy of the Personal Data we hold relating to you.
- The right to require us to rectify any inaccurate Personal Data about you without undue delay.
- The right to request us to erase any Personal Data we hold about you in circumstances such as where it is no longer necessary for us to hold the Personal Data or, in some circumstances, if you have withdrawn your consent to the processing.
- The right to object to us processing Personal Data about you such as processing for direct marketing.
- The right to request a restriction of the processing of your Personal Data.
- The right to data portability which allows you to move copy or transfer Personal Data from one organisation to another.
- The right not to be subject to a decision based solely on automated decision-making including profiling (subject to certain statutory restrictions).

Please note that these rights are not absolute rights and may be subject to statutory restrictions. You may exercise any of the above rights by contacting our **[Data Protection Officer OR Data Protection contact point]** at **[insert contact details]**

> For law firms to indicate which applies to your law firm: Refer to the Law Society GDPR Guide for guidance on whether your firm requires a DPO www.lawsociety.ie/intellectual-property--data-protection-law

Where our processing of your Personal Data is based on your consent to that processing (e.g. photographs for marketing), you have the right to withdraw that consent at any time, but any processing that we have carried out before you withdrew your consent remains lawful.

You may make a complaint with respect to our processing of your Personal Data to the Data Protection Commission.

Changes to this Data Protection Policy

We may update our Data Protection Policy from time to time. We will notify you of any changes that affect you as a Staff member.

Contact us

If you like to exercise any of your data protection rights or if have any questions about this Data Protection Policy, please contact us:

- By email: **[insert email]**
- By phone: **[insert phone number]**

Part 2

This section sets out your data protection obligations as Staff. It provides an overview of data protection definitions and principles. It then details your obligations when dealing with Personal Data while working with us.

Data Protection definitions and principles

Below is an outline of data protection principles as set out in the EU General Data Protection Regulation ("**GDPR**").

1. Data protection terms

Data is information, which is stored electronically, on a computer, or in certain paper-based filing systems.

Personal Data means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Restriction of processing means the marking of stored Personal Data with the aim of limiting its processing in the future.

Profiling means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

Filing system means any structured set of Personal Data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller.

Recipient means a natural or legal person, public authority, agency or another body, to which the Personal Data are disclosed, whether a third-party or not. However, public authorities which may receive Personal Data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Third-party means a natural or legal person, public authority, agency or body other than the Data Subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process Personal Data.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

Personal Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Genetic data means Personal Data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Biometric data means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person.

Data concerning health means Personal Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Representative means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27 of the GDPR, represents the controller or processor with regard to their respective obligations under the GDPR.

Supervisory authority means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR.

Special categories of Personal Data and Sensitive Personal Data includes information 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.

2. Data protection principles

All Staff must familiarise themselves with the key data protection principles set out below. Where a member of Staff becomes aware that one or more of these principles is not being complied with, they should bring it to the attention of the **[insert contact details]**.

2.1 Personal Data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("**lawfulness, fairness and transparency"**) - **Eg informing our firm's clients how we use their data via our Privacy Policy on the web site**,

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) of the GDPR, not be considered to be incompatible with the initial purposes ("**purpose limitation"**) - **Eg Using our clients' data in ways they would reasonably expect**,

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("**data minimisation"**) - **Eg Only using what client data we need and no more**,

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("**accuracy"**) - **Eg updating clients' data on our records in a timely manner**,

e) 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; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("**storage limitation"**) - **Eg deleting pre-recruitment background checks on job candidates once hired (in line with the firm's Retention Schedule)**,

f) 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, using appropriate technical or organisational measures ("**integrity and confidentiality"**) - or the **Security** principle – **Eg Using secure servers to store our clients' data**.

DATA PROTECTION OBLIGATIONS

As a law firm, we must comply with the GDPR (General Data Protection Regulation 2016/679) relating to how we handle Personal Data. As part of compliance with this regulation and other legal requirements, Staff have obligations when handling Personal Data within the firm.

Staff must comply with the following rules:

1. Staff must collect, access and process **only information** that is **required for their own specific work purposes.**
    a. E.g. a fee earner working on a conveyancing file must not access files that are not relevant to the project e.g. sensitive family law files.
    b. Eg Staff may only share client data, internally or externally, on a need-only basis.
2. Staff must ensure that all Personal Data is only **used for work related purposes**.
    a. Eg contact details for a client or opposing counsel cannot be used for any other purpose other than what is specified in our Privacy Notice.
    b. Eg Staff must not send client data to or from their own personal devices (unless with express authorisation from a Partner).
3. Staff must only collect and process Personal Data to the extent that it is **required for** the **specific purpose(s)** as set out **in our Privacy Notice** (on the firm's web site). In each section of the Privacy Notice, the specific purpose is indicated.
4. Staff must make sure that all **Personal Data** that is **collected** from any person is **relevant for the specified purpose.**

    E.g. we need contact details to correspond with our clients; we may need relevant health information for litigation purposes. However, while we might need to know about a client's trade union membership in advising on an employment matter, asking them for such information on a conveyancing matter may be irrelevant and excessive.
5. Staff must ensure that Personal Data held by the firm is kept accurate and up to date. When a client informs us of any changes to their personal details, Staff must ensure to update the client's file/profile in a timely manner.
6. We will only hold Personal Data for as long as is necessary and in accordance with our data retention policy. Staff must comply with all instructions relating to deletion/ confidential shredding etc.
7. Staff must be cognisant of requests for data received by them from any party in any form. Data Subjects have certain rights as outlined in Part 1 of this Data Protection Policy. As a firm we must respect and enable these rights, applying the relevant restrictions. If you receive a request from someone (by phone, email, post or in person) to exercise data protection rights, please immediately contact our **[Data Protection Officer OR Data Protection contact point]** at **[insert contact details]**

- ***For law firms to indicate which applies to your law firm: Refer to the Law Society GDPR Guide for guidance on whether your firm requires a DPO www.lawsociety.ie/intellectual-property--data-protection-law***
- Do not acknowledge or respond to the request before engaging with the contact point. The firm only has a short period of time to respond to Data Subject Rights requests, so please **treat this as urgent**.

8. We take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. We have put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Staff are obliged to follow and comply with these security measures as set out in [**law firm to specify policy/policies by name].** These measures include, but are not limited to, the following technical, physical and organisational measures.

   Technical Measures

   All Staff are required to:
   - Use only Firm-approved devices, software, and cloud services for the processing of personal data.
   - Ensure that devices are password-protected and, where supported, encrypted;
   - Ensure that email attachments containing sensitive/special category data (e.g., a client's health data) are encrypted or password protected.
   - Lock screens when leaving a workstation unattended.
   - Use strong, unique passwords for all systems containing personal data and not share login credentials.
   - Enable multi-factor authentication (MFA) where available.
   - Report immediately to **[insert contact point]** any loss or theft of a device used to access Firm data; and
   - Not use personal email accounts or consumer-grade file-sharing services (e.g., personal Dropbox, WhatsApp) to transmit client personal data.

   Physical and Organisational Measures

   All Staff are required to:
   - Store physical files containing personal data in locked cabinets when not in use.
   - Not remove physical files from the office without prior authorisation.
   - Dispose of physical documents containing personal data using cross-cut shredding or a secure confidential waste service.
   - Be alert to the risk of 'shoulder surfing' or unauthorised viewing of screens in public spaces.
   - Not discuss confidential client information in public areas; and
   - Clear your desk at the end of each working day.
   - Always verify bank details by phone using a trusted number before transferring funds (e.g. paying a supplier or transferring funds in a conveyancing matter).

9. Staff are required to act to minimise the likelihood of data breaches.

   A Personal Data breach is any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:

   - Sending a document containing personal data to the wrong recipient by email or post.
   - Loss or theft of a laptop, phone, or USB drive containing personal data.
   - Ransomware or other cyberattack affecting systems containing personal data.
   - Accidental deletion of data without backup; and
   - Unauthorised access to a client file by a member of staff with no legitimate need.

   Article 33 GDPR requires a data controller (in this case our law firm) to notify the DPC of a breach likely to result in a risk to the rights and freedoms of data subjects within 72 hours of becoming aware of the breach. Certain high-risk breaches must also be notified to affected data subjects under Article 34 GDPR.

10. Staff must immediately contact **[Data Protection Officer OR Data Protection contact point]** at **[insert contact details]** if they become aware of any breach or potential breach. The 72-hour clock begins when any member of staff first becomes aware of the breach. The firm may need to take immediate action to prevent unlawful access to our systems, so please treat this as urgent.

11. Staff must not engage new third-party services or software that will process personal data without prior approval from **[Data Protection Officer OR Data Protection contact point]**. This includes cloud-based practice management tools, AI-assisted drafting tools, e-signature platforms, and HR software. Personal Data will only be transferred to a Data Processor (for e.g. cloud-based practice management tools) if they agree to comply with those procedures and policies, or if they put in place adequate measures.

12. Staff must limit the sharing of Personal Data with third parties. Personal Data should be shared with third parties only on a need-to-know basis and only to the extent necessary for the purpose in question. This applies equally to sharing within a group of firms, barristers, counsel's chambers, expert witnesses, and opposing parties in litigation. Particular care is needed, for example, when forwarding email threads to check the entire content of the email thread before sending.

13. All Staff are required to complete all data protection training provided by the firm. Failure to complete such training within the prescribed period may be treated as a disciplinary matter.

14. All Staff are referred to the Law Society GDPR Guide for further assistance and guidance (on the Law Society web site).

15. All Staff must comply with this Data Protection Policy **[law firm may wish to specify additional related policies here by name].** Any breach of these policies may result in disciplinary action.

If you have any questions or concerns about data protection, please contact [**Insert contact details**]. If in doubt, ask!

Schedule 1

We have set out below a list of categories of third-party Data Processors with whom we share your data.

[Add or delete as relevant to your law firm]

Categories of recipients

- Cloud Services Providers
- Payroll Providers
- IT Service Providers
- Email Service Providers
- Practice Management System Providers
- Accounting/Tax Services Providers
- Confidential Waste Disposal Providers
- Document Management Providers
- Archiving/Storage Providers
- eSignature Service Providers
- Data Room Service Providers
- CCTV Providers
- Web Providers

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

Law Society of Ireland,
Blackhall Place,
D07 VY24
E solicitorservices@lawsociety.ie
W www.lawsociety.ie