THE LAW SOCIETY OF IRELAND

DATA PROTECTION POLICY

Version Number:	2
Date:	31 August 2018

CONTENTS

Section **PAGE**

Version Control and Responsibility for Maintaining the Data Protection Policy

The following people are responsible for maintaining this Data Protection Policy:

Head of F&A/Head of IT – Final Approval of all Revisions

Deirdre Byrne F&A – Providing Updates

Version Control

Version Number	Author	Purpose/Change	Date Adopted
2	F&A Department/McCann Fitzgerald	Update to Appendices	31 August 2018

Section 1 - General

1. About this Policy

1.1 The purpose of this policy is to outline the obligations of the Law Society of Ireland (the "**Law Society**") under applicable Data Protection Law, and to describe the steps to be taken to ensure compliance with those obligations. This document should be read in conjunction with the related policies as listed in Appendix 2 – Related Policies and Procedures that the Law Society maintains regarding compliance with applicable Data Protection Law.

1.2 This policy applies to the Law Society's Officers, Directors, executives (or other persons occupying a similar status or performing a similar function), employees and any other person who is subject to the Law Society's supervision and control (which may include consultants, advisors, temporary employees or other persons that are designated accordingly) (collectively, "**Employees**").

1.3 It is the responsibility of all Employees to comply with this policy. Failure to comply with this policy may result in the defaulting Employee being subject to disciplinary action, up to and including summary dismissal or termination of contract, as applicable.

1.4 If an Employee has any queries in relation to this policy, including regarding the scope of the policy and/or any related policies or procedures, please contact the Privacy Officer at dataprivacy@lawsociety.ie

2. General Policy Statement

2.1 Data Protection Law confers rights on individuals regarding their 'personal data' and imposes obligations on persons who process personal data. In the course of its business, the Law Society processes personal data relating to various categories of individuals, including Employees, solicitors, trainees, exam candidates, Law School contributors, members of the public etc.. In all such circumstances, it is the Law Society's policy to ensure that it processes such personal data in accordance with relevant Data Protection Law and the terms of this policy.

2.2 This policy relates to 'personal data'. Personal data is, broadly speaking, information relating to an identified or identifiable natural person (such as a name or an identification number). The legal definition of 'personal data', together with definitions of other key terms in relation to Data Protection Law, such as 'controller' and 'processor', are set out in Appendix 1 to this policy.

2.3 Personal data does not include contact details for corporate entities that happen to relate to an employee or other representative of that corporate entity. Examples of data which would not be regarded as personal data on this basis include: names, email addresses and telephone numbers of contacts of corporate bodies or solicitor partnerships. In addition, where such contact details have been provided to the Law Society in one corporate context, they may be used by the Law Society in another, related corporate context without being regarded as personal data. It is important to note, however, that business contact details may be regarded as personal data if the Law Society uses them to contact the individual in the individual's personal capacity – i.e. in the context of the individual's private life or personal career. Employees should avoid using corporate contact data for reasons other than the Law Society's official business.

3. The General Data Protection Regulation

3.1 Data Protection Law in the EEA is governed primarily by the General Data Protection Regulation (EU/2016/679) (the "**GDPR**"). The GDPR imposes significant compliance obligations on "controllers" such as the Law Society, and the Law Society could be subject to significant penalties for non-compliance with such obligations. All Employees should be mindful of data protection obligations when carrying out any activities that involve dealing with personal data.

3.2 The GDPR is supplemented by national legislation and by guidance published by competent regulatory authorities. This policy is kept under review and updated in light of such legislation and guidance as and when it is published and becomes applicable.

Section 2 – Data Protection Principles

1. Data Protection Principles

As a controller, the Law Society must comply with the following key data protection principles in relation to personal data:

(a) Obtain and process personal data lawfully, fairly and in a transparent manner;

(b) Process personal data for only specified, explicit and legitimate purposes;

(c) Ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

(d) Keep personal data accurate and, where necessary, keep it up to date;

(e) Retain personal data for no longer than is necessary for the purpose or purposes for which it is acquired;

(f) Keep personal data safe and secure;

(g) Be responsible for, and be able to demonstrate compliance with, obligations under applicable Data Protection Law; and

(h) Comply with requests from data subjects to exercise their data protection rights.

Details on how the Law Society complies with these principles in practice are set out below.

2. Obtain and process personal data lawfully, fairly and in a transparent manner

2.1 For personal data to be obtained fairly, data subjects must be provided with certain information, generally at the time at which the personal data is obtained. It is the Law Society's policy to do so by setting out the relevant information in an appropriately worded Data Privacy Statement and to provide this to data subjects at the time that data is collected, where it is possible to do so. The information that needs to be provided to data subjects includes: the identity and contact details of the controller; the purposes and legal basis for the processing activities; the potential recipients of personal data; and, where the personal data may be transferred to a non-EEA country, the safeguards which have been adopted in relation to such transfer. Employees should contact the Privacy Officer at dataprivacy@lawsociety.ie for further information in the event that their operation requires a Data Privacy Statement.

2.2 For personal data to be processed fairly, the Law Society must be in a position to rely on one of a range of 'legal grounds' that are set under relevant Data Protection Law. The Law Society generally relies on the following bases:

- 'legitimate interests' basis

- ‘processing necessary for the performance of a contract’ basis and
- ‘compliance with a legal obligation’ basis.
- Personal data that is processed incidentally in dealing with suppliers is processed on a ‘legitimate interests’ basis.
- Employees should contact the Privacy Officer at dataprivacy@lawsociety.ie if they require further information in relation to the legal basis for processing personal data.

2.3 The GDPR specifies certain “**special categories** of personal data” which require particular protection. These categories are personal data relating to:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data and
- data concerning health, sex life or sexual orientation.

2.4 In order for special categories of personal data to be processed fairly (unless exemptions which are set out under relevant Data Protection Law apply) the Law Society ensures that, in addition to one of the ‘legitimising grounds’ applying, at least one ‘**special legitimising condition**’ is met. The ‘special legitimising conditions’ for special categories of personal data are more limited than the ‘legitimising grounds’ for ordinary categories of personal data. The main ‘special legitimising condition’ for processing data relating to Employees is that the processing is required for compliance with obligations or exercising rights in the field of employment and social security and social protection law and the main special legitimising condition outside of the employment context is where the data subject has given their explicit consent to the processing of special categories of data relating to them. Employees should contact the Privacy Officer at dataprivacy@lawsociety.ie if they have any queries in relation to a special category of personal data.

2.5 The Law Society may only process personal data relating to criminal convictions or offences when authorised by law. The Law Society occasionally needs to process such data. The Law Society ensures that it has a valid legal basis under applicable EU or national laws for carrying out such processing, e.g. under the Solicitors Act 1954 - 2015. Employees should contact the Privacy Officer at dataprivacy@lawsociety.ie if they have any queries in relation to personal data relating to criminal convictions or offences.

3. Processed personal data for only specified, explicit and legitimate purposes

3.1 The Law Society only processes personal data for a purpose(s) that is specific, lawful and clearly stated. Employees are reminded that they should not collect information

about people routinely and indiscriminately without having a sound, clear and legitimate purpose for doing so. The Law Society's practice is to keep personal data for lawful purposes which are set out in the Data Privacy Statements that are made available to Employees, solicitors, trainees, exam candidates, Law School contributors, members of the public etc..

3.2 If Employees obtain personal data relating to other Employees, solicitors, trainees, exam candidates, Law School contributors, members of the public etc. for a particular purpose then, subject to limited exceptions, the data should not be used or disclosed for any other purpose that is incompatible with that for which it was obtained. The Law Society's practice is to process personal data only in accordance with the purposes set out in its Data Privacy Statements or as otherwise required or permitted by applicable law. If Employees are planning any new activity or implementing any new initiative that will involve changing the way that the Law Society collects or processes personal data, they should contact the Privacy Officer at dataprivacy@lawsociety.ie will in turn be responsible for the updating of the Data Inventory and will decide whether a Data Protection Impact Assessment or Privacy Impact Assessment should be carried out in accordance with the criteria referred to in Section 4 – Documenting and Monitoring Compliance.

4. **Ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed**

Personal data should not be collected or kept if it is not needed or on the off-chance that a use might be found for it in the future. The Law Society's practice is to ensure that it collects and keeps only such personal data as is necessary for the purposes set out in its Data Privacy Statements. The types of information about individuals which the Law Society collects and keeps are periodically reviewed to ensure compliance with this requirement, and information that is no longer required is deleted in accordance with the Law Society's Data Retention Policy (to be developed in Phase 2 of GDPR project) See Section 4 – Documenting and Monitoring Compliance, for further details.

5. **Keep personal data accurate, complete and up-to-date**

The Law Society seeks to ensure that the personal data it holds is at all times accurate, complete and up to date. The Law Society requests Employees, solicitors, trainees, exam candidates, Law School contributors, members of the public etc. and other third parties to notify it of changes to their personal data (e.g. upon a change of address). The Law Society takes every reasonable step to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay in accordance with the procedures set out in Section 4 – Documenting and Monitoring Compliance.

6. **Retain personal data for no longer than necessary for the purpose(s) for which it is acquired**

Unless legally required (for example to comply with employment or anti-money laundering legislation) the Law Society does not retain personal data in a form that permits the identification of data subjects indefinitely. The Law Society's policy is to ensure that its record retention, archiving and destruction practices give effect to this principle. Data Retention Policy (to be developed in Phase 2 of GDPR project) for details of the periods for which the Law Society retains the various categories of records that it holds.

7. **Keep personal data safe and secure**

7.1 The Law Society ensures that personal data is 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. The Law Society's practice is to ensure that Employee and other third party access to personal data which is held by the Law Society is restricted on a 'need to know' basis. To the extent that any third party processes personal data on behalf of the Law Society, the Law Society ensures that there is a written agreement in place which includes, among other things, appropriate security obligations regarding such personal data (see Section 3 – Dealing with Third Parties).

7.2 The security of the Law Society's IT systems is under the overall responsibility of the IT Section. All Employees and other third parties who have access to the Law Society's IT systems are subject to security and acceptable use policies which outline their responsibilities in using the Law Society's IT Systems. Further details regarding the technical and security measures that are implemented by the IT Section. are set out in the Employee Handbook and IT Policy.

8. **Be responsible for, and be able to demonstrate compliance with, obligations under applicable Data Protection Law**

The Law Society takes its responsibility to comply with applicable Data Protection Law seriously and maintains this policy and the practices referred to in this policy for this purpose. The Law Society also ensures that it can demonstrate its compliance with its obligations under applicable Data Protection Law. The Law Society achieves this by maintaining the records, policies and procedures referred to in Section 4 – Documenting and Monitoring Compliance and listed in Appendix 2.

9. **Comply with requests from data subjects to exercise their data protection rights**

9.1 Under Data Protection Law, individuals (such as Employees, solicitors, trainees, exam candidates, Law School contributors, members of the public etc.) have the following rights in relation to the processing of their personal data (subject to certain limited exceptions):

(a) The right to access personal data. Data subjects have the right to be provided with a copy of their personal data along with certain details in relation to the processing of that personal data.

(b) The right to information. Data subjects have the right to be provided with certain information, generally at the time at which their personal data is obtained. The Law Society complies with this obligation via its Data Privacy Statements.

(c) The right to rectification. Data subjects have the right to have inaccurate personal data that a controller holds in relation to them rectified.

(d) The right to object to and restrict processing. Data subjects have the right to require that a controller restricts its processing of their data in some circumstances, and have the right to object to the processing of their data in certain circumstances.

(e) The rights in relation to automated decision making. Data subjects have the right not to be subjected to processing which is wholly automated and which produces legal effects or otherwise which significantly affects an individual, and which is intended to evaluate certain personal matters, such as creditworthiness or performance at work, unless one of a limited number of exemptions applies.

(f) The right to be forgotten. Under certain circumstances a data subject has the right to request the erasure of their personal data.

(g) The right to data portability. Under certain circumstances, the Law Society is required to provide a data subject with a copy of their personal data in a structured, commonly used and machine readable format.

9.2 The Law Society is obliged to comply with any requests by a data subject to exercise the above rights within strict timelines imposed under Data Protection Law (generally one month). As such, if an Employee receives such a request They should notify their Section Head/Manager who should notify the Privacy Officer at dataprivacy@lawsociety.ie without delay. In general, requests by current or former Employees are processed through the HR Section and requests by solicitors, trainees, exam candidates, Law School contributors, members of the public etc. are processed by the relevant department.

9.3 Further details on the procedures to be adopted on receipt of a request from a data subject to exercise their data protection rights can be found in the Law Society's Data Subject Request Guidance.

Section 3 – Dealing with Third Parties

1. Engaging Processors

1.1 A processor is a third party that processes personal data on behalf of the Law Society. Common examples include companies that provide outsourced services such as payroll services providers, IT support service providers, cloud hosted software providers, file storage agents, confidential waste disposers, mailshot dispatchers, event managers etc. If a third party has access to personal data that belongs to or is controlled by the Law Society in order to provide a service to the Law Society, then the third party is acting as a processor to the Law Society.

1.2 If the Law Society provides access to personal data to a third party, but that third party uses the personal data for its own purposes, this will be a controller to controller transfer (see below for further details).

1.3 Section [TBC] of the Data Inventory sets out details of the processors that are engaged by the Law Society. The details of processors in the Data Inventory must be kept up to date in accordance with the procedure set out in Section 4 – Documenting and Monitoring Compliance.

1.4 Prior to engaging processors, the Law Society:

(a) undertakes due diligence to ensure that it is appropriate to engage the processor; and

(b) ensures that it puts in place a Data Processing Agreement in writing with the processor that complies with the requirements under applicable Data Protection Law.

1.5 Relevant Departments will be responsible for issuing Data Processing Agreements. A record of the arrangements that the Law Society has in place with third party processors will be kept by the Privacy Officer. For further details of the records the Law Society retains in relation to its dealings with third party processors, see Section 4 - Documenting and Monitoring Compliance.

2. Controller to Controller Transfers

2.1 In certain circumstances the Law Society transfers personal data relating to Employees, solicitors, trainees, exam candidates, Law School contributors, members of the public etc. and other third parties to third parties, or allows third parties to have access to such personal data, on a controller to controller basis. This means that the third party will process such personal data for their own purposes and not on behalf of the Law Society. By way of example, this will occur in the following circumstances:

(a) Pensions – When Employee data is provided to a pension service provider, the trustee(s) of the pension will be a controller in relation to such data. This data is then processed by the pension trustees (or the pension service provider) for the purposes of administering the pension; For further information see Data Privacy Statements for Law Society of Ireland Pension and Life Assurance (Defined Benefit) Scheme and Law Society of Ireland Defined Contribution Plan.

(b) Health Insurance – When Employees are provided with health insurance, the health insurance provider (e.g. [Vhi, Laya etc.]) will be a controller in relation to the Employee data that is used to administer the insurance;

(c) Audits – Where a third party is granted a right to audit the Law Society, and the audit is carried out on behalf of that third party (i.e. it is not an internal audit, or an audit by a third party that is requested by the Law Society), any personal data (e.g. relating to the Law Society's Employees, solicitors, trainees, exam candidates, Law School contributors, members of the public etc.) that is processed in the context of such audits is processed by the auditing party as a controller;

(d) Public Bodies – The Law Society is required by law to transfer certain personal data to public bodies (e.g. the Revenue Commissioners). The public body becomes a controller in relation to any personal data that it receives.

(e) Other examples of Controllers whom the Law Society of Ireland share data with are Barristers, Solicitors, Independent Adjudicator, Solicitors Disciplinary Tribunal and Grant Bodies.

2.2 Where there is a controller to controller transfer, the transferee is primarily responsible for complying with data protection obligations (i.e. the Law Society is not responsible for ensuring that a transferee of personal data complies with that transferee's data protection obligations). The Law Society's policy is to seek the consent to the transfer of their data, except for where the transfer is required by law or is otherwise permitted under applicable law to take place in the absence of consent. [Details of controller to controller transfers are set out in section [TBC] of the Data Inventory.] In the event that the transfer involves a transfer of data outside of the EEA, paragraph 3 below applies.

3. **Transfers of Personal Data Outside the European Economic Area (EEA)**

3.1 Under Data Protection Law, the Law Society may not (save where one of a limited number of exemptions applies) transfer personal data outside of the EEA to any third country, unless that third country is deemed by the European Commission to provide an adequate level of protection in relation to the processing of personal data. This prohibition on transfers outside the European Economic Area will not apply, amongst other things, if:

(a) The data subject has explicitly consented to the transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) The transfer is necessary for the performance of a contract between the controller and data subject, or the implementation of pre-contractual measures taken at the data subject's request;

(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) The transfer is necessary for the establishment, exercise or defence of legal claims;

(e) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(f) A data transfer agreement, in the form approved by the European Commission or a data protection supervisory authority, has been executed by the exporter of data and the importer based outside of the EEA;

(g) The transfer is made pursuant to a Code of Conduct that has been approved under applicable Data Protection Law, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights;

(h) The transfer is made pursuant to a certification mechanism that has been approved under applicable Data Protection Law, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights;

(i) The data importer is subject to a framework approved by the European Commission to facilitate transfers (e.g. the EU – U.S. Privacy Shield); or

(j) A multi-national organisation has developed a set of "Binding Corporate Rules" governing the transfer of data to third countries and such rules have been approved by the relevant data protection supervisory authorities.

3.2 If it is necessary for the Law Society to transfer personal data, of which the Law Society is a controller, to another legal entity that is located in a country outside the EEA which is not recognised as providing adequate levels of protection for personal data, then the Law Society must ensure that it can rely on one of the exemptions referred to above. This may arise in relation to transfers of personal data to third parties who are not members of the Law Society (e.g. external service providers). Details of the Law Society's transfers of personal data outside of the EEA are set out in the Data Inventory, together with details of the basis on which those transfers are made.

3.3 Employees should contact the Privacy Officer at dataprivacy@lawsociety.ie for guidance if they are engaging in any activity or project which involves the transfer of personal data outside of the EEA.

Section 4 – Documenting and Monitoring Compliance

1. Ensuring Compliance

As noted above in Section 2, paragraph 8, the Law Society is obliged to put in place policies and procedures to ensure that it can demonstrate its compliance under Data Protection Law. The Law Society achieves this by maintaining the records referred to in Appendix 2 to this policy, and the Data Inventory and in accordance with the monitoring of compliance set out in this section.

2. Data Inventory

2.1 The Law Society is required to maintain an inventory of the personal data that it holds (both as a controller and a processor). The inventory must include the following details about the Law Society's processing of personal data:

(a) details of the controller(s);

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) details of transfers of personal data to a third country, including the identification of that third country;

(f) where possible, time limits for retention; and

(g) where possible, a description of the technical and organisational security measures that are undertaken to protect the data.

2.2 The Law Society's Data Inventory is maintained by the Privacy Officer and reviewed on an annual basis. If Employees are planning any new activity or implementing any new initiative that will involve changing the way that the Law Society processes personal data, they should contact the Privacy Officer at dataprivacy@lawsociety.ie so that such information can be added, if necessary, to the Data Inventory.

3. Privacy by Design and Default

3.1 Two of the key principles under Data Protection Law are that data protection compliance shall be implemented by design and by default, this means:

(a) **Data Protection by Design** - Data protection by design is the notion that the methods and purposes of the processing of personal data are designed, from the beginning, with data protection in mind. The principle requires the Law Society to implement both technical and organisational measures that will guarantee and protect the privacy of data subjects. The Law Society seeks, where possible, to implement and practice methods of data minimisation (which could include, where feasible, the pseudonymisation of personal data). Other methods of data protection by design include staff training and audit and policy reviews in the context of data protection.

(b) **Data Protection by Default** - The Law Society implements appropriate technical and organisational measures to ensure that, by default, only personal data which is necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of its processing, the period of its storage and their accessibility. In particular, such measures ensure that by default a data subject's personal data is not made accessible, without the data subject's consent, to an indefinite number of natural persons.

3.2 The Law Society ensures data protection by design and data protection by default through, among other things, following the procedures set out in paragraph 4 below, whenever it implements a new project.

4. **Data Protection Impact Assessments**

4.1 The Law Society is obliged to ensure that a Data Protection Impact Assessment ("**DPIA**") is undertaken before commencing any processing that is likely to result in a "high risk" to data subject's rights and freedoms. Examples under GDPR of such processing are the "large scale" processing of sensitive personal data or profiling activities.

4.2 A DPIA must contain at least the following details:

(a) a description of the envisaged processing operations and the purposes of the processing;

(b) an assessment of the necessity and proportionality of the processing;

(c) an assessment of the risks to the rights and freedoms of data subjects; and

(d) the measures envisaged to address the risks that have been identified and to demonstrate compliance with the GDPR.

4.3 The Law Society also considers whether a Privacy Impact Assessment ("**PIA**") is necessary when it engages in changes to its processing of personal data that do not require a DPIA. Both DPIAs and PIAs are carried out before the processing activity in question is commenced.

4.4 Each DPIA and PIA that is carried out by the Law Society is submitted to the Privacy Officer at dataprivacy@lawsociety.ie for review once it is completed and at regular intervals thereafter. The default period for such reviews is every 3 years, but shorter periods may be stipulated depending on the subject of the DPIA or PIA.

5. **Accuracy**

5.1 The Law Society ensures that personal data is accurate and kept up-to-date. The Law Society takes every reasonable step to ensure that any personal data that is inaccurate or out of date, having regard to the purposes for which it is processed, is erased or rectified without delay in accordance with the following procedures:

(a) The Law Society stipulates in its Data Protection Statements for Employees, solicitors, trainees, exam candidates, Law School contributors, members of the public etc. and third parties (where appropriate) a requirement to notify

the Law Society of any changes to their personal data (e.g. a change in an individual's address) and records any updates that are notified to it;

(b) The Law Society reviews its Data Inventory annually.

6. Training

6.1 The Law Society ensures that Employees whose roles involve the processing of personal data are made aware of and, when necessary, receive training in respect of data protection law and principles. Records of data protection training completed by Employees are maintained as part of their personnel files or within Human Resources training records.

7. Storage Limitation

7.1 Personal 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 is processed. Guidance from supervisory authorities has indicated that personal data should never be kept on a "just in case" basis, unless there are reasonable grounds for expecting that such information may be required. As such, personal data should not be collected or kept if it is not needed and/or on the off-chance that a use might be found for it in the future.

7.2 To ensure compliance with the principles of Data Protection Law (and any applicable statutory requirements in respect of the retention of records), the Law Society's practice is to:

(a) ensure that it collects and keeps only such personal data as is necessary for the purposes set out in its Data Privacy Statements. The types of information about individuals the Law Society collects and keeps are periodically reviewed to ensure compliance with this requirement;

(b) retain such personal data only for as long as required for the purposes for which it is processed (or for any applicable statutory retention period). The Law Society maintains and implements a Data Retention Policy (to be developed in Phase 2 of GDPR project) to achieve this;

(c) periodically review and update as necessary the Law Society's Data Retention Policy to ensure that it provides for retention periods that are relevant and appropriate having regard to statutory requirements, guidance from supervisory authorities, etc.; and

(d) periodically carry out Society-wide audits and spot checks to ensure that the Law Society adheres to the retention periods Data Retention Policy

Section 5 – Marketing

1. Compliance with Data Protection Law

1.1 The Law Society may at times invite Employees, solicitors, trainees, exam candidates, Law School contributors, members of the public etc.and other individuals to events, or send them articles on relevant products/services/courses/developments etc. In some circumstances such communications may fall within the definition of "unsolicited direct marketing" under European law (see paragraph 2.3 below).

1.5 When undertaking direct marketing that involves the processing of personal data the Law Society must ensure that it processes such personal data in accordance with the general principles set out in Section 2 above. The Law Society must also ensure that it provides data subjects with the right to object to the processing of their personal data for the purposes of marketing. The Law Society complies with these obligations by ensuring that appropriate consent wording is included in its Data Privacy Statements that it uses when collecting personal data or seeking consent.

2. Compliance with Restrictions on Direct Marketing

2.1 In addition to complying with the general principles of applicable Data Protection Law, the Law Society must also ensure that any electronic direct marketing that it undertakes complies with the provisions of applicable ePrivacy Law, which is currently set out in Directive 2002/58/EC (the "**ePrivacy Directive**") as implemented into local law and which will, soon after May 2018, be set out in a new EU Regulation (the "**ePrivacy Regulation**").

2.2 In summary, ePrivacy Law requires a person who uses personal data for direct marketing purposes to notify data subjects of such proposed use of their personal data when their data is collected and, depending on the method of communication to be used, to afford data subjects an opportunity to 'opt-out' or, in some cases, to obtain an express 'opt-in', to such use of their personal data.

2.3 Employees should be aware that the definition of "*direct marketing communications*" in the proposed ePrivacy Regulation is very broad and could potentially apply even to business advertising sent to corporate contacts. The proposed definition, as at May 2018, is as follows:

> "'*direct marketing communications' means any form of advertising, whether written or oral, sent or presented to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail message, SMS, etc*.

2.4 Employees who carry out any direct marketing activities that might fall within the scope of ePrivacy Law, should contact the Privacy Officer at dataprivacy@lawsociety.ie

Section 6 – Data Security

1. **Data Security**

1.1 The Law Society implements appropriate technical and organisational measures to ensure a level of security appropriate to the risks to personal data that may arise in connection with the processing activities the Law Society undertakes. Such measures include:

(a) the encryption of personal data where appropriate;

(b) ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) ensuring the ability to restore access to personal data in a timely manner in the event of a physical or technical incident;

(d) regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

1.2 In assessing the appropriate level of security the Law Society takes account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

1.3 All Employees, solicitors, trainees, exam candidates, Law School contributors, members of the public etc and other third parties who have access to the Law Society's IT systems are subject to security and acceptable use policies which outline their responsibilities in using the Law Society's IT Systems. Further details regarding the technical and security measures, and the organisational security measures, that are implemented by the Law Society IT Section are set out in the IT Security Policy.

2. **Data Security Incidents (Data Breaches)**

2.1 Regardless of the measures that are taken in accordance with the above paragraph and related policies, there is always a risk of data security breaches or incidents arising. Data security breaches or incidents may range from relatively minor incidents, which do not actually result in unauthorised disclosure, loss, destruction or alteration of personal data, to major security incidents, such as the loss or theft of devices, such as laptops, which contain personal data or hacking of systems.

2.2 The GDPR defines a 'personal data breach' as 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.

2.3 It is essential that all data security incidents are reported to Head of IT, Infrastructure and Cyber Security Manager/Privacy Officer without delay, and that the following procedures are followed.

2.4 Head of IT, Infrastructure and Cyber Security Manager/ Privacy Officer will:

- consider whether the incident constitutes a personal data breach.
- if the incident does constitute a personal data breach, consider whether a notification to the supervisory authority (Data Protection Commissioner) is required.
- if the incident does constitute a personal data breach, consider whether a notification to the data subject(s) is required.
- take such steps as are required to stop, contain or mitigate the effects of the data security incident and ensure that appropriate steps are taken in response to the incident, including the putting in place of new policies and procedures where necessary.

2.5 Where a personal data breach occurs it must be reported to the competent supervisory authority without delay and, where feasible, not later than 72 hours after the Law Society becomes aware of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The ultimate decision on whether to report the breach will rest with the Privacy Officer.

2.6 Where a personal data breach is likely to result in a high risk to the rights and freedoms of affected data subjects, then those data subjects must also be notified without undue delay. When assessing whether there is a high risk to data subjects it is important to bear in mind that one of the core purposes for notifying data subjects is to help data subjects take steps to protect themselves from any negative onsequences of the breach. Therefore if, for example, the personal data which is the subject of the breach was encrypted, notification to data subjects would not be necessary. In addition, where the notification of individual data subjects would involve a disproportionate effort a general public communication or similar measure will be sufficient. The ultimate decision on whether to advise a data subject(s) of a breach will rest with the Privacy Officer. The responsibility to advise the data subject, if deemed necessary by the Privacy Officer, rests with the relevant Section/Department.

2.7 Notifications to supervisory authorities must include the following information:

(a) a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) the name and contact details of the Head of IT, Infrastructure and Cyber Security Manager/ Privacy Officer a description of the likely consequences of the personal data breach; and

(c) a description of the measures taken or proposed to be taken by the Law Society to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

2.8 Notifications to data subjects must include the information set out at (a), (b) and (c) above.

2.9 Head of IT, Infrastructure and Cyber Security Manager/ Privacy Officer will also ensure that an appropriate record of the data security incident as well as any associated communications, are maintained in the IT & Data Security Incident Log.

Section 7 – Compliance and Enforcement

1. **Data Protection Officer**

The Law Society considers that the appointment of a DPO is not necessary for the following reasons:

(a) the Law Society is not a public authority or body;

(b) the Law Society's core activities do not consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; and

(c) the Law Society does not process special categories of personal data or personal data relating to criminal convictions and offences on a large scale.

The Law Society has appointed TBC as its Privacy Officer.

2. **Supervisory Authority**

2.1 Each country in the EEA has a "**Supervisory Authority**" that oversees compliance with Data Protection Law. In Ireland the Data Protection Commission (the "**DPC**") is the relevant Supervisory Authority.

3. **Enforcement, Sanctions and Penalties**

3.1 It is important that all Employees comply with this policy and related policies and procedures, as a breach of Data Protection Law could result in serious consequences for the Law Society. Such consequences could include the following:

(a) **Investigations, Audits and Criminal Penalties**

The DPC has a wide range of investigation and enforcement powers, including the powers to investigate complaints, to carry out an audit of an organisation's compliance with Data Protection Law and the power to issue enforcement notices setting out steps which must be taken to rectify breaches of Data Protection Law. Failure to comply with enforcement actions by Supervisory Authorities may result in a criminal offence;

(b) **Fines**

In addition to their investigation and enforcement powers for certain breaches of the GDPR, the DPC can levy fines of up to the greater of:

4% of annual worldwide turnover of the relevant undertaking. For the Law Society as at May 2018 this is €1.4m.

or €20 million.

3.2 All communications from the DPC, must be forwarded immediately to the Privacy Officer at dataprivacy@lawsociety.ie

4. **Interactions with Data Protection Commission**

All interactions with the DPC will be recorded by the Privacy Officer.

Appendix 1 - Definitions

The following definitions are, in some cases, modified versions of definitions which are set out in the relevant Data Protection Law. For the exact wording of the relevant definition, please see the relevant Data Protection Law.

Automated means is, broadly speaking, processing using a computer or other electronic device.

Data means information in a form which can be processed. It includes both data processed by automated means and manual data.

Controller or data controller means any person who, either alone or with others, controls the purpose and means of the processing of personal data. Controllers can be either legal entities such as companies, government departments or voluntary organisations, or they can be individuals.

Processor or data processor means a person who processes personal data on behalf of a controller, but does not include an employee of a controller who processes such data in the course of his/her employment.

Data Protection Law means the General Data Protection Regulation (EU Regulation 2016/679) and any applicable national implementing legislation.

Data subject means an individual who is the subject of personal data.

Manual data means information that is recorded as part of a 'filing system', or with the intention that it should form part of a 'filing system'. 'Filing system' means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographic basis.

Personal data means data relating to a living individual who is or can be identified either directly or indirectly, including by reference to an identifier (such as a name, identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental economic, cultural or social identity of a person). This can be a very wide definition, depending on the circumstances.

Processing means performing any operation or set of operations on personal data including: (a) recording the data; (b) collecting, organising, structuring, storing, altering or adapting the data; (c) retrieving, consulting or using the information or data; (d) disclosing the data by transmitting, disseminating or otherwise making it available; or (e) aligning, combining, restriction, erasing, or destroying the data.

Special Categories of Personal Data means personal data relating to an individual's: racial or ethnic origin; political opinions or religious or philosophical beliefs; trade union membership; genetic or biometric data processed for the purpose of uniquely identifying a natural person; physical or mental health, including in relation to the provision of healthcare services; sex life or sexual orientation: individuals have additional rights in relation to the processing of any such data.

Appendix 2 – Related Policies and Procedures

	Policy /Procedure	**Kept by Business Unit**
1	Data Inventory	Finance & Administration Department
2	Data Processors Listing	Finance & Administration Department
3	Data Release Policy	Finance & Administration Department
3	Data Breach Policy	Finance & Administration Department
4	Record Retention Policy	Currently under review August 2018
5	Controller to Controller Policy	Currently under review August 2018
6	Photography and Filming Policy	Currently under review August 2018
7	Induction and Employee Handbook	HR Department - under review August 2018
8	CV Policy	HR Department - under review August 2018
9	IT Policy	IT Department

Appendix 3 – Data Privacy Statements

	Data Privacy Statement	**Owner:**
1	Preliminary Exams and Fe1 Exams	Paula Sheedy, Education.
2	PPC1 and PPC2	Geoffrey Shannon, Education.
3	Traineeship	Ian Ryan, Education.
4	QLTT	Catherine Byrne, Education.
5	Trainees and Solicitors for admission to the Roll of Solicitors	Philomena Whyte, Education.
6	Barristers for admission to the Roll of Solicitors	Philomena Whyte, Education.
7	CPD Regulation	Rosemarie Hayden, Education.
8	Diplomas	Freda Grealy, Education
9	Law Society Professional Training	Attracta O'Regan, Education
10	Employees	Rowena Bottrill, Human Resources
11	Job Applicants	Rowena Bottrill, Human Resources
12	Law Society of Ireland Pension and Life Assurance (Defined Benefit) Scheme	Rowena Bottrill, Human Resources
13	Law Society of Ireland Defined Contribution Plan	Rowena Bottrill, Human Resources
14	Complaints and Client Relations - Solicitors	Linda Kirwan, Regulation
15	Complaints and Client Relations - Claimants	Linda Kirwan, Regulation
16	Claims on Compensation Fund	Seamus McGrath, Regulation
17	Practice Inspections	Seamus McGrath, Regulation
18	Practice Closures	David Mulvihill, Regulation
19	Practice Certificates	Sorcha Hayes, Regulation
20	Four Courts room bookings	Paddy Caufield, Four Courts
21	Council and Committee Members	Under review/rollout pending September 2018
22	Law School Contributors	Under review/rollout pending September 2018

Appendix 4 – Guidance Notes

	Guidance Notes	**Updated**
1	Handling Medical Records	September 2018
2	Handling CVs	September 2018
3	File Transfers	September 2018
4	Direct Marketing	September 2018
5	Storage of Credit Card Information	Under Review September 2018
5	Gathering Data	September 2018
6	Keeping Data	September 2018
7	Disclosing Data	September 2018
8	Disclosing Data to third parties	September 2018