An tÚdarás Clárúcháin Maoine
Property Registration Authority

Property Registration Authority

Data Protection Policy

2022

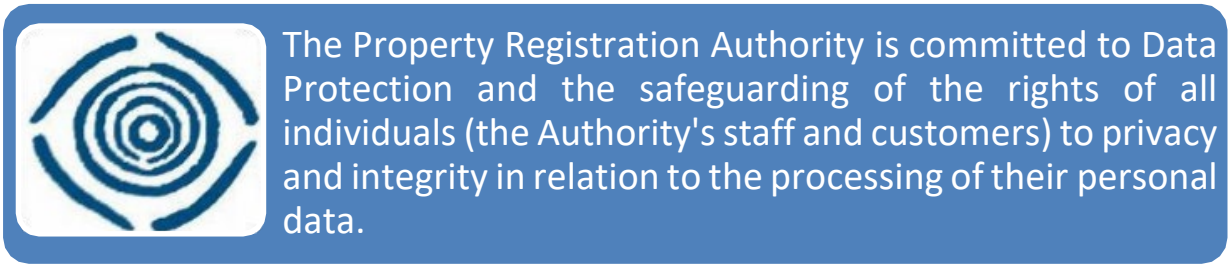
Contents

1. Policy Overview 1
1.1 Scope 1
1.2 General Data Protection Regulation (GDPR) 1
1.3 Data Protection Act 2018 2
1.4 Complying with Data Protection legislation 2
1.5 Personal data held by the PRA 2
1.6 Incidents occurring pre-GDPR 2
1.7 Principles of the General Data Protection Regulation 3
2. Rights and Responsibilities 4
2.1 Rights of the Data Subject 4
2.2 Responsibilities for Heads of Divisions 5
2.3 Responsibilities of all Staff 6
2.4 Responsibilities of the DPO 6
2.5 Responsibilities of the DPU 6
2.6 Responsibilities of the Data Protection Network (DPN) 6
2.7 Responsibilities relating to Data Governance 7
2.8 Responsibilities of the Data Governance Steering Group (DGSG) 7
2.9 Responsibilities of the Data Officer (DO) 7
2.10 Data Protection Impact Assessments (DPIAs) 7
2.11 Privacy by Design and Default 7
3. Training and Awareness 8
4. Data Protection Commission (DPC) 8
5. Data Protection Review and Audits 8
6. Data Breach Management 8
7. Data Subject Access Requests 9
7.1 Data Exempt from Data Protection Legislation 9
7.2 Responsibility of Staff in Data Subject Access Requests 9
7.3 Further information 10
8. Retention 10
8.1 Human Resources files 10
9. CCTV 10
10. The use of ICT in the PRA for staff 11
11. Data Protection and the PRA Websites 11
12. Data Sharing Policy 12

Appendix 1 - Office Notices 13
Appendix 2 - Key Definitions 14
Appendix 3 - Useful Contacts 16
Appendix 4 - Additional Resources 17

Name of Document	Property Registration Authority - Data Protection Policy 2022
Owner of Document	Data Protection Unit
Approved by	Management Board
Date of Approval	13/01/2022
Date of Amendments	16/05/2022
Nature of Amendments	Minor changes, primarily to reflect records management updates
Date of Formal Review	Q3 2023

1. Policy Overview



This Data Protection Policy is a living document which is subject to change and should be read in conjunction with the PRA's Data Protection Strategy and the PRA's Data Strategy. This Policy will be reviewed regularly in light of any legislative or other relevant developments. It will also be subject to comprehensive, formal review every 18 months.

Data Protection is the manner in which we safeguard the right to privacy of our customers and staff and the manner in which this personal data is processed. Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. The definition is also technology neutral. It does not matter how the personal data is stored – on paper, on an IT system, on a CCTV system etc. The Data Protection Policy, as set out below, provides guidance on the administration of personal data across the PRA.

1.1 Scope

The Policy covers personal data and special categories of personal data, held in both manual / hard copy and automated / electronic formats, (as defined by Article 4 of the GDPR) held by the PRA in relation to data subjects. Personal data and special categories of personal data will be treated with equal care by the PRA and will be referred to as 'Personal Data' in this Policy, unless specifically stated otherwise.

1.2 General Data Protection Regulation (GDPR)

The GDPR requires organisations to be more transparent about how they process individuals' data and to ensure that the processing has a legal basis. There are six different legal bases on which personal data may be processed:

1. Consent.
2. Contract.
3. Legal obligation.
4. To protect the vital interests of the data subject or of another.
5. Task carried out in the public interest or in the exercise of official authority vested in the controller.
6. Legitimate interest.

As a public body, the PRA has a legal obligation to fulfil its statutory function and, as such, processing of customer data is for the purposes of completing, and also maintaining, the public Land Register under the Registration of Title Act 1964, Registration of Deeds and Title Act 2006, and the Land and Conveyancing Law Reform Act 2009. The Land Registration is also governed by the Land Registration Rules 2012, Land Registration (Fees) Order 2012.

The GDPR seeks to ensure that organisations consider how the data is used, put control measures in place to mitigate the risk of breaches and document how such breaches are to be managed to minimise the effect it may have on the data subject(s).

1.3 Data Protection Act 2018

From 25th May 2018, all processing of personal data and the protection of data subject rights fall under the EU regulation (The GDPR). The Data Protection Act 2018 incorporates Ireland's national implementation measures required under the GDPR and created a new regulatory framework for the enforcement of Data Protection laws in Ireland. Organisations must comply with both pieces of legislation.

1.4 Complying with Data Protection legislation

Data Protection legislation applies whether you are working in the office, blended working or remote working. Data Protection is a key issue with remote working in the PRA, in particular regarding the risks involved in potential removal of hard copy documents from the PRA buildings.

For any blended working or remote working operations, Data Protection Impact Assessments (DPIAs) should be carried out for proposed new projects/initiatives or changes in procedure.

Please note that DPIAs should be carried out regardless of the working regimes, be it working in the office, blended working or full remote working.

1.5 Personal data held by the PRA

The PRA collects personal data of customers only for purposes of completing and maintaining the public (National) Land Register. Personal data includes, but is not limited to, names, addresses, lodging party and applicant details. There may also be some official documents held at the point of registration, such as bank details, affidavits, correspondence, application forms etc.

1.6 Incidents occurring pre-GDPR

Incidents occurring before the implementation of the GDPR will be assessed under the Data Protection Acts 1988 and 2003.

1.7 Principles of the General Data Protection Regulation

The principles, as set out in the GDPR, are binding on the PRA as a data controller and any failure to observe them is a breach of Data Protection legislation. It is the responsibility of every staff member to follow all of the principles. The policies and procedures in the PRA are designed to ensure compliance with the following principles:

- Personal data shall be processed **lawfully, fairly and in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency').

- Personal data shall be 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), not be considered to be incompatible with the initial purposes ('purpose limitation').

- Personal data shall be **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation').

- Personal data shall be **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').

- Personal data shall be **kept in a form which permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed; 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) 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').

- Personal data shall be **processed in a manner that ensures appropriate security of the personal data,** including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. Rights and Responsibilities

2.1 Rights of the Data Subject

A data subject has the right to obtain a copy, clearly explained, of any personal data relating to him or her kept on computer or held in manual format in a relevant filing system. This right applies to staff and to customers of the PRA. Data subject rights are enforced through Articles 15-22 of the GDPR which are set out below:

- **Right of access by the data subject (Article 15)**
  Data subjects have the right to access the data that the PRA holds on them. To do so, an application form should be submitted along with proof of identity (ID) and address so that it may be authenticated. Where an access request is being refused by the PRA, the reasons for the refusal will be outlined to the data subject (see Subject Access Request Office Notice).

- **Right to rectification (Article 16)**
  The PRA makes every effort to ensure that the personal data of data subjects is accurate and up to date. However, if a data subject believes that their personal data is not accurate or relevant they can contact the PRA's Data Protection Unit (DPU). They should set out clearly the personal data involved and the reasons why they consider it to be inaccurate. The PRA will either amend the data without undue delay or explain to the data subject why we will not do so.

- **Right to erasure (right to be forgotten) (Article 17)**
  Data subjects have the right, in certain circumstances, to have their data erased or no longer processed. However, this right cannot interfere with the statutory functions of the PRA. Should a data subject wish to have their data erased, they should email the DPU and the request will be considered. They should set out clearly the personal data involved and the reasons why they consider that the data should be erased. The PRA will either grant the request without undue delay or explain why it will not do so.

- **Right to restriction of processing (Article 18)**
  In certain circumstances a data subject has the right to request that the PRA restricts processing of their personal data. However, this right cannot interfere with the statutory function of the PRA. Data subjects may apply either in writing or by email to the DPU so that the request may be considered. Data subjects should clearly set out the personal data involved and the reasons why they consider processing should be restricted. The PRA will either grant the request without undue delay or explain why it will not do so.

- **Notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19)**
  Access to the public Land Register is available through the PRA's online application, landdirect.ie, or by application to one of its public counters, or by post to the PRA offices. Such information is subject to change as the Land Register and Register of Deeds are dynamic and constantly changing records. Where feasible, changes including rectification, erasure of personal data or restriction of processing will be notified to the relevant parties.

- **Right to data portability (Article 20)**
  Data subjects have the right to data portability unless it applies to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

- **Right to object (Article 21)**
  Data subjects have the right to object to certain processing, unless the processing is carried out for the performance of a task undertaken for reasons of public interest or in the exercise of official authority vested in the controller. Where such an objection is received, the PRA will assess each case on its merits. Data subjects also have the right to object to direct marketing. On occasion, the PRA has reason to communicate with its customers via email. Such emails are only issued to customers who have actively opted in to receive them and who may at any time choose to opt out.

- **Automated individual decision-making, including profiling (Article 22)**
  Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling which produces legal effects concerning them or significantly affecting them. Applications for registration submitted to the PRA are not subject to automated processing.

The PRA takes Data Protection very seriously and will endeavour to ensure that a data subject's personal data is protected at every stage. However, a data subject has the right to query and or complain either through the Data Protection Officer (DPO) or Data Protection Commission (DPC). The data subject will be informed of their right to bring their complaint to the DPC and their contact details.

2.2 Responsibilities for Heads of Divisions

Heads of Divisions are responsible for ensuring implementation of the Policy in their respective Divisions and will, if required, need to be able to demonstrate implementation to the DPO.

2.3 Responsibilities of all Staff

All members of staff have been made aware of their responsibility to ensure that personal data is kept safe and secure against unauthorised access, alteration, disclosure or disposal of personal data. All staff should review the relevant Office Notices and any queries should, in the first instance, be directed to the Data Protection Administrator. Staff must also comply with the provision of information, where requested, for Data Subject Access Requests.

2.4 Responsibilities of the DPO

Under the GDPR, specific rules are applicable to public sector bodies including the mandatory designation of a DPO. The DPO in the PRA is responsible for:

- Monitoring compliance with Data Protection legislation and ensuring that all obligations are met to safeguard the rights of customers and staff.
- Overseeing the functions of the DPU and providing guidance.
- Acting as a contact point and providing cooperation with the DPC.
- Reporting to the Management Board and the CEO on Data Protection matters.

2.5 Responsibilities of the DPU

In addition to the appointment of the DPO, the DPU was established in 2017 and now forms part of the Quality and Compliance Division. The DPU manages Data Protection in the PRA, as well as having a wider Data Governance role in the PRA. The DPU has responsibility for:

- Monitoring that all Data Protection policies, Strategies and Office Notices relating to Data Protection/Governance are reviewed and updated on a regular basis.
- Providing advice where requested as regards the Data Protection Impact Assessments and monitoring that such assessments are completed to an appropriate standard.
- Investigating Data Breaches.
- Processing Data Subject Access Requests.
- Ensuring that Bulk Data applications are compliant with the PRA's requirements and appropriate for processing.
- Providing advice on Data Protection matters from staff, board members and other stakeholders.
- Monitoring that the Record of Processing Activity (ROPA) is updated regularly.

2.6 Responsibilities of the Data Protection Network (DPN)

To assist the DPU in its work, and to ensure effective communication between the DPU and all of the divisions in the PRA, a DPN has also been established. This network comprises representatives from all areas of the PRA and is instrumental in assisting the DPU with mapping the processes around personal data in the PRA and identifying and mitigating the risks associated with those processes.

2.7 Responsibilities relating to Data Governance

In addition to responsibilities relating to data privacy and protection, there is a wider context for data management and governance in the PRA. This data governance remit incorporates the PRA's role as guardian and steward of the data entrusted to us from customers, as well the maintenance and protection of the public Land Register, other records and archives. The PRA's approach to data governance is encapsulated in its Data Governance Principles. Further details of the PRA's approach to, and ambition for, its data can be seen in the PRA's Data Strategy.

2.8 Responsibilities of the Data Governance Steering Group (DGSG)

The PRA's DGSG was established in 2019 and comprises representatives with particular responsibilities for data management across a range of functions. It has a key role in providing oversight to how the PRA manages its data, as well as driving adherence to best practice and data governance principles across the organisation. The group drafted the new PRA's Data Strategy and continue to work through the actions as set out in the Data Strategy.

2.9 Responsibilities of the Data Officer (DO)

The Data Governance Unit (part of the OGCIO) have established a network of Data Officers (DO) across the public service. The DO role was created in order to ensure that Public Service bodies can manage and share data in line with their legislative responsibilities under the Data Sharing and Governance Act 2019. The DO will play a role in managing Data Sharing Agreements (DSAs) in the PRA and will ensure the PRA adheres to the new rules and processes for data sharing.

2.10 Data Protection Impact Assessments (DPIAs)

As set out in the PRA's Project Management Policy, all projects require a DPIA to be completed, as well as other initiatives and changes where data is involved. Project Managers are encouraged to engage early in the life cycle of a project so that any Data Protection issues can be resolved and where required, changes made to the project plan to insure compliance. Heads of Function, Project Sponsors and Project Managers working on projects involving personal data should consult with the DPU as necessary.

2.11 Privacy by Design and Default

The PRA has embedded data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage by the requirement to carry out a DPIA on any change that impacts the way that it processes personal data. This helps to ensure better and more cost-effective protection for individual data privacy.

Data Protection by default involves making choices to implement processing that is the minimum necessary by default to achieve the desired objective. Specifically the amount of personal data collected, the extent of processing, the period of retention and who has access to the data will all be reviewed at an early stage.

3. Training and Awareness

The DPU has responsibility for raising awareness of the PRA's obligations under the legislation and provides a number of avenues for staff to stay informed of the policies and procedures in place to protect the rights of both colleagues and customers. The channels for this awareness raising include mandatory staff information sessions, mandatory online training courses for all staff, monthly updates in bulletins, posts on the PRA's 'Rainbow' channels, specific emails, posters and intranet banners on an on-going basis. Other channels will also be used as appropriate.

4. Data Protection Commission (DPC)

The DPC is responsible for upholding the rights of individuals and enforcing the obligations upon data controllers. Members of the Commission (Commissioners for Data Protection) are appointed by Government, but the Commission is independent in the exercise of its functions. Individuals who feel their rights are being infringed can make a formal complaint to the Commission. The matter will be investigated and the necessary steps will be taken to resolve it.

Further information on the DPC can be found at www.dataprotection.ie.

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2
D02 RD28
Ireland

5. Data Protection Review and Audits

The DPU, in the course of its duties and/or at the request of the DPO, may carry out a review and/or audit in a particular area, function or location of the PRA to ensure ongoing compliance with Data Protection legislation.

The DPC may also carry out a review or audit of the PRA at any stage.

The PRA's approach to GDPR and Data Protection is also subject to audit by Internal Audit or 'Quality and Compliance' Audit, and any findings may give rise to revision of this policy.

6. Data Breach Management

Under Article 85 of the GDPR, organisations are obliged to notify the supervisory authority within 72 hours of becoming aware of a breach and to minimise the material or non-material damage caused to the data subject(s) affected. It is therefore important that staff notify the DPU immediately upon the potential occurrence of a breach so that it may be investigated appropriately. Please refer to the PRA's Breach Management Policy on the Data Protection

page, http://opra/strategycorporate/data-management/data-protection/for further details.

7. Data Subject Access Requests

Under Article 15 of the GDPR, data subjects have a right to access their personal data and to be informed of the type of data held. A Data Subject Access Request can be made in writing (e- mail or written letter) addressed to the Data Protection Administrator, Property Registration Authority, Chancery Street, Dublin 7 (e-mail: DataProtectionUnit@prai.ie, "Data Subject Access Request" should be quoted in the subject header).

Staff requests for personal data access may go directly to the DPU or to Local HR, and should include reference to their personnel number.

7.1 Data Exempt from Data Protection Legislation

There are certain documents which may not be included in a subject access request reply, such as:

- **Folios and Maps which form part of the Public Register**
  The Irish Land Register is a public record and any person, as provided for under Rule 165 of the Land Registration Rules 2012, may inspect the folios and maps, on payment of the prescribed fees. In this regard, Data Protection legislation, as provided for under Section 60(7)(m) of the Data Protection Act 2018, does not apply to the data contained in the folio given that the land register is a public register.

- **Completed Applications for Registration – Instruments**
  Access to Land Registry Instruments is governed by Rule 159 of the Land Registration Rules 2012 and, therefore, access to an Instrument (i.e. documents lodged in respect of a completed application for registration) cannot be granted under Data Protection legislation as part of a Data Subject Access Request.

- **Court Registered files**
  All records created in relation to court proceedings are considered court records and therefore fall solely under the control of the courts. Accordingly, it is a matter for the Judge to decide whether, and in what format, access to the record is to be provided.

7.2 Responsibility of Staff in Data Subject Access Requests

Staff must ensure that if they receive a Data Subject Access Request, it is sent directly to the DPU (DataProtectionUnit@prai.ie) for the attention of the Data Protection Administrator, so that it can be completed within the required timeframe.

Staff should assist in requests for documents as soon as possible so that the Data Protection

Administrator can meet the one month turnaround target. A two month extension is available under Article 12, sub section 3 of the GDPR for requests that are complex or voluminous. In this instance, the data subject should still be informed within one month and an explanation should be provided as to why the extension is required. Any delay in the completion of the Data Subject Access Request could result in a sanction from the DPC which could take the form of an administrative fine (amongst others).

7.3 Further information

Officers should be professional and objective in the type of language used in the course of their work – particularly in relation to personal data. As a basic rule of thumb, you should not use any expression/comment in an e-mail, (including internal e-mail), written letter, on IM systems (Rainbow and Starleaf), in memos etc. that you would not wish to have released to an individual as part of his/her personal data under a Data Subject Access Request or that you would not wish to see appearing in the public media as a result of an FOI request.

Please refer to the Subject Access Request Office Notice for further details.

8. Retention

Documents submitted for the purposes of registering a property are subject to Rule 152(3) and held indefinitely as they form part of the Public Register.

Other documents, such as copy folios and copy instruments may be disposed of in line with the PRA's Record Retention Schedule and following the PRA's Disposal Procedures. Approval for disposal must be given by the PRA Records Manager and the Certifying Officer.

8.1 Human Resources files

Local HR retains both hardcopy and electronic Personnel files. These personnel files are to be held for the lifetime of the staff member and their surviving beneficiaries and then may be disposed of according to the retention schedule. For staff members that transfer to other Government Departments, Local HR will forward on the hardcopy personnel files to the Local HR in the transferring Department.

In general, line managers should not hold documents relating to staff in hardcopy or electronically. Records relating to staff such as sick leave, flexi leave etc. should be processed through HR Shared Services.

9. CCTV

Please note that CCTV (closed-circuit television) is used in the premises of the PRA for the purposes of ensuring the security of the premises, records or other property and to capture images of intruders or of individuals damaging property, interfering with PRA property or

removing goods without authorisation. Office Notice 5 of 2017 provides further details of the use of CCTV in the PRA.

10. The use of ICT in the PRA for staff

There is a suite of Office Notices detailing the responsibilities of staff and their use of ICT facilities. These notices can be found in the Internal Procedures Office Notices section. To summarise, in terms of Data Protection, at a minimum staff should ensure that:

- the intended recipient has been correctly entered when sending emails;
- information contained in emails does not relate to a third party which could give rise to a data breach;
- passwords are compliant with best practice; and
- screens are locked when staff are away from their desks.

11. Data Protection and the PRA Websites

The PRA provides online services to its customers in order to fulfil its statutory duty of providing access to the public Land Register. The full privacy policy of the PRA regarding the use of the PRA website and the data collected can be found here https://www.prai.ie/privacy-policy/. However, in summary:

- The PRA will not collect any personal information about individuals during their visit to the websites without clear consent.
- Any information which is provided by individuals during their visit will be treated with appropriate standards of security and confidentiality and in strict accordance with the terms of the prevailing Data Protection legislation.
- Visitors to these sites cannot be identified through the collection of technical information and it is only used to assist in providing and developing an efficient service and to make the sites more effective.
- The PRA does not use cookies or web beacons on its websites, apart from temporary "session" cookies which enable a visitor's web browser to remember which pages have already been visited during that particular session.
- Credit or debit card information of customers is not retained on the site, rather it is securely transferred to a secure online payments provider.

12. Data Sharing Policy

The PRA may also provide bulk data from the Land Register to other Government Departments and Agencies in accordance with legislation. Access to bulk extraction may also be provided subject to application as set out below.

There are three provisions whereby a customer may submit an application to the PRA for data extracts from the Land Register. It should be noted that the provision of such data may be subject to certain terms and conditions and may involve the signing of a Data Sharing Agreement, including under the Data Sharing and Governance Act 2019.

Applications to the PRA for data extracts may be made pursuant to one of the following application types:

- Land Registry Fees Order 2012 (Schedule Item 22).
- PSI Regulations S.I. 525/2015.
- Other Specific Statutory provision.

Further information on data extraction can be found on Appendix 7b of the PRA's Mapping Guidelines.

Appendix 1 - Office Notices

The following notices provide additional detail on the Data Protection Policies of the PRA:

Information and Communication Technology Facilities: Acceptable Usage Policy	IP (ICT) Office Notice 4/2021
Protocol for the Reporting of Potential Money Laundering to An Garda Síochána	IP (CS) Office Notice 5/2021
Policy on the Use of Laptop Computers	IP (ICT) Office Notice 1 of 2020
Protocol for Data Disclosure to An Garda Síochána	IP (CFU) Office Notice No. 2 of 2020
Clean Desk and Workspace Policy	IP (CS) Office Notice 4 of 2020
Personal Data of Staff	IP (CS) Office Notice 1/2019
Security of Personal Data in Transit	IP (CS) Office Notice 2/2019
Building Security & Visitors	IP (CS) Office Notice 3/2019
Management and Filing of Instruments	IP (CS) Office Notice 5 of 2019
Management of Dealings	IP (CS) Office Notice 6 of 2019
Passwords and Security	IP (ICT) Office Notice 4/2018
Security and Use of Smartphone	IP (ICT) Office Notice 6/2018
Subject Access Request	IP (CS) Office Notices 7/2018
Personal Data of Customers	IP (CS) Office Notice 10/2018
CCTV and Operating Procedures	IP (CS) Office Notice 5/2017
Monitoring of Staff & Use of ICT Facilities	IP (ICT) Office Notice 6/2010

Appendix 2 - Key Definitions

The following are the list of key definitions in Data Protection legislation. Please refer to Article 4 of the GDPR for additional definitions.

Term	Definition
Data Subject	The individual as referred to in the Data Protection Acts. This includes the PRA's customers and staff.
Personal Data	Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information. For example, a customer is readily identifiable from his policy number. Staff may be identifiable from his or her role title.
Special Categories of Personal Data	Means personal data consisting of information as to: ○ the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject; ○ whether the data subject is a member of a trade union; ○ the physical or mental health or condition, sexual orientation or sexual life of the data subject; ○ the commission or alleged commission of any offence by the data subject; and ○ any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings; ○ any processing of genetic or biometric data in order to uniquely identify the person.
Data Protection Commission	The supervisory authority for the purposes of the Data Protection Regulation and the Directive. The Commission will consist of up to three members (Commissioners). It is independent in the performance of its functions and monitors the lawfulness of processing of personal data.
Commissioner for Data Protection	Each member of the DPC is a Commissioner for Data Protection. The person who is the Data Protection Commissioner immediately before the establishment day will be a Commissioner for Data Protection. They are responsible for upholding the rights of individuals as set out in the Data Protection Bill, and enforcing the obligations upon data controllers.
Data Controller	The company or organisation that collects and processes personal data. For the purposes of Data Protection legislation, the PRA is a Data Controller.

Data Processor	The third party contracted to process personal data on behalf of the Data Controller. For example, the National Shared Services organisation and the PRA's third party administration providers.
Data Protection Officer	An expert on data privacy who works independently within an organisation to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Appendix 3 - Useful Contacts

Title	Name	Email	Phone Number
Property Registration Authority Staff and Roles			
Data Protection Officer	Aidan Timmins	Aidan.Timmins@prai.ie	01 804 8051
Data Protection Manager	James Barry	James.Barry@prai.ie	01 804 8158
Data Protection Administrator/Data Officer	Liz McDonnell	Liz.Mcdonnell@prai.ie	01 804 8039
Data Protection Support	Niamh Hayden	Niamh.Hayden@prai.ie	01 804 8433
Data Protection Commission			
Data Protection Commissioner	Helen Dixon	info@dataprotection.ie	01 7650100/ 1800437 737

Appendix 4 - Additional Resources

Full text of the General Data Protection Regulation

Rights of Individuals under the General Data Protection Regulation

Data Protection Act 2018

Data Protection Impact Assessments (DPIA)

Data Protection Commission

European Data Protection Board