Data Protection Policy

platform housing group

Scope of Policy

This policy sets out how Platform Housing Group (the Group) will ensure compliance with the legal requirements of the Data Protection Act (DPA), UK General Data Protection Regulations (UK GDPR), Data (Use and Access) Act, Privacy and Electronic Communication Regulation (PECR) and associated legislation that contains data protection related content.

Applicability

The policy guidance applies to you if you are an employee, a contractor, or a partner where you are processing personal data of employees, customers or other third parties on behalf of the Group.

1. Policy Statement

1.1 The policy sets out how the Group applies the data protection principles, recognises and responds to people's data rights and meets its accountability and governance obligations.

2. Context

2.1 This policy provides information about what policies, controls, processes, guidance, notices and training are in place to enable the achievement of service objectives.

Applying this policy will help develop the proficient data protection knowledge, skills and behaviours needed to operate efficiently, effectively, and lawfully when interacting with the customers, suppliers and partners.

2.2 It is integral to our Corporate Strategy Goals around People (work with our customers to improve what we do) and Data (utilise insights through accurate, robust and secure data).

2.3 It is foundational to our Group Values particularly People Matter, Own It and Be Brave.

2.4 It facilitates our ability to meet and measure up to the Regulator for Social Housing's Consumer Standards particularly the:

- Transparency, Influence and Accountability Standard
- Neighbourhood and Community Standard
- Tenancy Standard

2.5 It promotes the "positive data culture" sought by the Housing Ombudsman when they recommend Registered Providers implement improved knowledge and information management practices.

3. Aims and Objectives

3.1 The aims and objectives of the policy is to identify the requirements of the data protection legislation and to provide guidance on how the Group interprets and responds to those requirements.

3.2 The Information Commissioner, who oversees compliance and promotes good practice, requires all data controllers who process personal data to be responsible for their processing activities and comply with 7 key DPA principles set out in the UK GDPR.

Those 7 principles are also closely aligned with the rights of Data Subjects.

By adhering to these principles and respecting the rights of its customers, employees and other stakeholders, the Group will operate in a more efficient and effective manner leading to improved trust and satisfaction with its services.

3.3 Through the Accountability Principle the UK GDPR places the responsibility firmly on the Group to take responsibility for what it does with personal data and to have appropriate measures, roles, contracts, risk assessments and records in place to demonstrate compliance.

3.4 The remainder of this section is set out as an index to enable the reader to jump to more detailed guidance in the Policy Outline section below.

3.4.1 What are the UK GDPR seven key principles of data protection that I should adhere to?

3.4.2 What lawful purposes are there for processing and when should I rely on consent?

3.4.3 What about sensitive data such as health, disabilities, Equality, Diversity and Inclusion (EDI) and gender reassignment?

3.4.4 What about Criminal Offence Records?

3.4.5 What rights do data subjects have and how will we respond to them?

3.4.6 What is a Data Subject Access Request?

3.4.7 What is the Right To Be Informed (Privacy Notices)?

3.4.8 What is a Right to Correction?

3.4.9 What is the Right to Erasure?

3.4.10 What is a Right to Restrict Processing?

3.4.11 What is the Right to Object?

3.4.12 What rights are there where automated decisions and profiling take place?

3.4.13 What about the ethical use of Personal Data?

3.4.14 What is the Right To Data Portability?

3.4.15 What does the Accountability Principle require the Group to have in place?

4. Policy Outline

4.1 The Group is committed to compliance with data protection legislation. It regards the lawful and secure processing of personal information as fundamental to operating efficiently, in a non- discriminatory manner, offering excellent customer services and ensuring the highest confidence by customers in the integrity of our data processing systems.

4.2 **Data Protection Principles**

All personal data processing carried out by the Group should meet the **seven key principles** which lie at the heart of the general data protection regulations. These are set out in Article 5 of the UK GDPR and are listed below.

4.2.1 Article 5(1) requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals (**'lawfulness, fairness and transparency'**).
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('**purpose limitation**').
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation'**).
(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**').
(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; ('**storage limitation**').
(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**').

4.2.2 Article 5(2) adds the accountability principle:

"The controller shall be responsible for and be able to demonstrate compliance with Article 5(1). ('**accountability**')."

4.3 **Lawful Bases**

The UK GDPR sets out **6 lawful bases for processing personal data.** These are listed below.

4.3.1 At least one of these must apply whenever the Group processes personal data:

(a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
(b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
(d) **Vital interests:** the processing is necessary to protect someone's life.
(e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

4.3.2 The vast majority of personal data processing carried out will be for fulfilling the Group's lease and tenancy contract obligations.

From time to time the other lawful bases may apply dependent on the activity involved.

Legitimate Interest is common where we do not have a contractual arrangement with an individual but may need to complete investigations involving them or process data to fulfil our financial and governance obligations.

Consent will only be relied on in limited circumstances. These typically will be marketing activities, some processing of sensitive special category data or a one of piece of data processing where the other purposes cannot be relied upon.

4.3.3 **Special Category Data**

The Group is required to process special categories of personal data for numerous reasons including monitoring equality of opportunity or treatment, and to adjust service provision to meet the needs of an individual.

When processing health, disability and equality and diversity records the group will ensure that one of the following additional conditions are met in addition to the lawful purpose listed in 4.3.1.

These conditions are listed in Article 9 of the UK GDPR:

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law
(j) Archiving, research and statistics (with a basis in law)

When relying on conditions (b), (h), (i) or (j), the Group will also need to meet the associated condition in UK law, set out in in Part 1 of Schedule 1 of the DPA 2018.

When relying on the substantial public interest condition in Article 9(2)(g), the Group will also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

4.3.4 Where required, and in particular when relying on substantial public interest or employment, social security and social protection conditions, the Group should capture the activity in an Appropriate Policy Document

Additional procedural security is to be followed for transgender data subjects holding a Gender Recognition Certificate. Section 22 of the Gender Recognition Act 2004 establishes that it is an offence except in limited circumstances described in the legislation for a person to disclose information acquired in an official capacity about a person's application for a gender recognition certificate or about the gender history of a successful applicant.

4.3.5 **Criminal Offence Data**

In the course of its duties the Group will process the personal data of offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings.

The Group will rely on one of the specific conditions in paragraphs 10 (preventing or detecting unlawful acts) and 11 (protecting the public against dishonesty) of Schedule 1 of the DPA 2018 and capture the activity in an appropriate policy document and as part of the DPIA procedure.

4.4 Data Subject Rights

The Group recognises and will adhere to the data subject rights detailed in the UK GDPR which may or may not apply depending on the selected lawful bases for processing personal data.

It recognises requests can be both written and oral and can be made to any person in the organisation or its appointed data processors.

Requests will be managed via the Data Governance Team through appropriate controls and processes.

Appropriate proof of identity will be determined for any rights request.

Requests will usually be responded to within one calendar month. Where longer may be required the Data Subject will be informed.

Where a request is deemed to be excessive or manifestly unfounded the request may be refused and the data subject informed.

The Group will not apply a charge for Data Subjects to exercise these rights.

4.4.1 Data Subject Access Requests

We recognise that individuals have the right to obtain a copy of structured identifiable personal data held about them within the Group's electronic information systems and in relevant manual filing systems.

The Group may withhold, or redact, personal data where lawful exemptions may apply.

4.4.2 The Right to Be Informed (Privacy Notices)

The Group will provide individuals with information about the collection and use of their data and recognises this as meeting a key transparency requirement under UK GDPR.

Through publication of its Privacy Notice it will ensure that individuals are aware of the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with.

The Privacy Notice will be referred to at all key customer contact points involving processing personal data.

The Privacy Notice will be reviewed regularly to ensure it remains accurate, transparent, understandable and is easily accessible with clear and plain language.

4.4.3 The Right to Rectification

The Group recognises that data subjects have a right to have inaccurate personal data rectified, or completed if it is incomplete.

The Group may refuse, or partially refuse a request where it deems the personal data to be accurate.

4.4.4 The Right to Erasure (Right to Be Forgotten)

The Group recognises that in some circumstances data subjects have the right to have personal data that is available at the time of the request erased.

It recognises that this right can apply if:

- The personal data is no longer necessary in relation to the purposes for which it was originally collected or processed.
- Consent is identified as the lawful purpose for processing and the data subject withdraws their consent.
- Legitimate Interest is identified as the lawful purpose for processing, the data subject objects, and there is no overriding legitimate interest to continue this processing.
- The personal data is processed for direct marketing purposes and the individual objects to that processing.
- The personal data has been processed unlawfully.
- Where required, to comply with a legal obligation.

The Group recognises that it must inform other organisations of any erasures where it has disclosed information to them unless this is impossible or involves disproportionate effort.

The Group recognises that where technically feasible personal data should also be erased from backup systems.

4.4.5 The Right to Restrict Processing

The Group recognises that Data Subjects have the right to request the restriction of the processing of their personal data. That is to limit the way that the Group can use their data.

Restrictions will usually be time limited to address a particular issue with a Data Subject.

Data Subjects have the right to request the Group restrict the processing of their personal data in the following circumstances:

- They are contesting the accuracy of their personal data and the Group is verifying the accuracy of the data.
- The data has been unlawfully processed and they oppose erasure and requests restriction instead.
- The Group no longer need the personal data but the Data Subject needs the Group to keep it to establish, exercise or defend a legal claim.
- They have objected to the Group processing their data under the Legitimate Interest lawful purpose, and the Group are considering whether its legitimate grounds override those of the Data Subject.

Whilst responding to a Right to Restrict Processing, the Group shall quarantine the personal data and clearly flag that it should not be processed further pending the outcome of the query.

4.4.6 **The Right to Object**

The Group recognises that data subjects have an absolute right to stop their data being used for direct marketing and that it has no grounds to refuse that request.

The Group also recognises that a data subject may object to their processing if it is for:

- A task carried out in the public interest.
- The exercise of official authority vested in the Group.
- The Group's legitimate interests (or those of a third party).

In these circumstances, the Group will investigate the reason given for the objection and liaise with the Data Subject to determine an appropriate and lawful outcome.

4.4.7 **Rights Related to Automated Decision Making including Profiling**

The Group recognises that it must have safeguards and processes in place where Data Subjects may become subject to:

- automated individual decision-making (making a decision solely by automated means without any human involvement).
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The Group uses profiling to:

- find something out about individuals' preferences.
- predict their behaviour.

- make decisions about them.

Such profiling and automated individual decision making can lead to quicker and more consistent decisions.

Where automated decision making is carried out that has legal or similarly significant effects on a data subject the Group recognises that additional restrictions apply and that this type of decision making can only be carried out where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by domestic law applicable to the controller; or
- based on the individual's explicit consent.

Where such processing applies the Group will give the Data Subject clear information about the processing, have a simple way for them to request human intervention or to challenge a decision. It will also keep the system under regular review to prevent errors, bias and discrimination.

The Group will carry out a Data Protection Impact Assessment (DPIA) to consider and address the risks and necessary mitigations before we start any new automated decision-making or profiling.

4.4.8 **Ethical Use of Artificial Intelligence, Bots, Big Data, Machine Learning and Profiling**

The Group recognises that modern data processing and service delivery increasingly involves the use of artificial intelligence, machine learning, combining big data from the Internet of Things and profiling data aimed at improving service delivery, performance of our homes and meeting our Corporate Objectives.

The Group commits to reviewing the use of these technologies against an ethical framework and ensuring that ethics by design are incorporated into any DPIA completed for these technologies and that its Privacy Notice reflects these processing developments.

4.4.9 **The Right of Data Portability**

The Group recognises that data subjects have the right to obtain and re-use personal data they have provided for their own purposes across different services.

The right allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. This enables them to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.

In the event of any such requests, where feasible, the data will be provided in a structured, commonly used and machine-readable format. The information will be

provided free of charge and within one month of the request being received and verified.

We recognise that any requests to exercise this right will be rare and limited and will be processed by the Data Protection Officer

4.5 The Accountability Principle

Accountability is one of the 7 data protection principles. It makes the Group responsible for complying with UK GDPR and for demonstrating that ongoing compliance.

The Group demonstrates compliance through a data privacy framework that consists of:

- Adopting and implementing data protection policies.
- Taking a 'data protection by design and default' approach.
- Putting written contracts in place with organisations that process personal data on our behalf.
- Maintaining documentation of our processing activities.
- Implementing appropriate security measures.
- Recording and, where necessary, reporting personal data breaches.
- Carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests.
- Appointing a data protection officer.

4.5.1 Adopting and Implementing Data Protection Policies

The Group will adopt and maintain robust and comprehensive data protection policies in line with its processing activities. It will demonstrate implementation and adherence to those policies through awareness raising, training, monitoring and audits. These activities will be coordinated by the Data Protection Officer role detailed below in 4.5.8.

4.5.2 Adoption of a 'Data Protection by Design and Default' Approach

The Group will implement a data protection by design approach at key opportunities including:

- Process reviews.
- Service design reviews.
- Contract reviews.
- Database and document management system retirements.
- Project implementation.

4.5.3 Use of Contracts and Data Processing Agreements

Where the Group either contracts out the processing of personal data to a third party or processes personal data under contract for a third party we will ensure that appropriate data processing contract clauses are in place.

These contract clauses, or a separate data processing agreement, will include the following requirements of the data processor:

- Process the personal data only in accordance with documented instructions from the Data Controller.
- Ensure that those authorised to process the personal data observe confidentiality.
- Take appropriate security measures.
- Respect the conditions for engaging any other processor where applicable.
- Assist the controller by implementing appropriate technical and organisational measures.
- Delete or return all personal data to the controller at the contract end.
- Make available to the data controller all information necessary to demonstrate compliance with this policy and related regulations.
- Ensure that all employees who have access to personal data processed on behalf of the Group are fully trained in and are aware of their duties and responsibilities under the Act.
- Allow data protection audits to be undertaken by or on behalf of the Group.

4.5.4.1 Record of Processing Activities (Information Asset Register)

The Group will maintain an up-to-date record of processing activities undertaken which will contain the following information:

- The name and contact details, as applicable, of the controller, any joint controller, controller's representative and Data Protection Officer.
- The purposes of the processing.
- A description of the categories of data subjects and the categories of personal data.
- The categories of recipients to whom the personal data has been or will be disclosed.
- Any international transfers of personal data and the documentation of appropriate safeguards.
- The envisaged time limits for erasure of the different categories of data.
- A general description of the technical and organisational security measures implemented.

4.5.4.2 **Privacy Notice Content**

Through its Privacy Notice, the Group will provide data subjects with the following information:

- The identity and contact details of the Data Controller and representative.
- The contact details of the Group's Data Protection Officer.
- The purposes of the processing as well as the legal basis of the processing.
- The legitimate interests pursued by the controller or by a third party.
- The recipients, or categories of recipients, of the personal data, if any.
- Where the data controller intends to transfer the personal data to a third country and the existence of adequacy conditions where relevant.
- The period of time the data will be stored (see the Group's Data Retention Policy).
- The right to rectification, erasure, restriction or objection as applicable.
- The right to data portability (right to have personal data transmitted to another data controller) where relevant.
- The right to lodge a complaint with a supervisory authority e.g., the Information Commissioners Office (ICO).
- The consequences of the data subject's failure to provide data.
- The existence of automated decision-making, including profiling, as well as the anticipated consequences for the data subject.

4.5.5 **Implementing Appropriate Security Measures**

The Group will create, record and implement a suite of technical and organisational measures appropriate to the risk of the processing activity that ensures the confidentiality, integrity and availability of the systems and services that it uses.

These measures include information security policies, access controls, security monitoring and recovery plans. The Group will regularly assess these against the ISO 27001 standard.

4.5.6 **Recording and Reporting Personal Data Breaches**

A personal data breach refers to a data protection breach that results in the loss, destruction, alteration, unauthorised disclosure of, or access to, personal data. A record of all reported personal data breaches is maintained by the Group.

Reported incidents will be triaged and risk assessed by the Data Governance Team. Where required they will work with the Group's IT teams to investigate, manage and mitigate any risks.

Higher risk incidents will be escalated to the affected Senior Leadership/Executive Team level where necessary.

If a breach has been assessed as likely to result in a risk of adversely affecting individuals' rights and freedoms, it will be reported to the ICO within 72 hours. In addition, if a breach has been assessed as likely to result in a high risk to the rights and freedoms of individuals, the Data Subject(s) concerned must be informed directly, unless an exemption detailed in Article 34 applies or there is a requirement for us to communicate via an authorised representative or third-party.

4.5.7 Data Privacy Impact Assessments (DPIA)

The Group recognises that DPIAs are an essential accountability tool and are an integral part of taking a privacy by design approach.

The Group will carry out a DPIA when using new technologies or datasets where the processing is likely to result in a high risk to the rights and freedoms of individuals.

DPIA findings will be submitted to the Data Protection Officer for an independent assessment of the compliance risk and advice on any mitigating actions. Mitigating actions will be incorporated into respective project risk and action logs for implementation.

The Data Protection Officer will coordinate all DPIAs completed in the business and appropriate higher risk activities will be notified to Executive Risk Committee.

4.5.8 Appointment and Role of the Data Protection Officer (DPO)

Given the scale and scope of its personal data processing activities the Group shall appoint a DPO who will:

- Inform and advise the controller, its employees, and any associated processors about their obligations to comply with the UK GDPR and other relevant data protection laws such as Part 3 of the Act;
- Monitor compliance with data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits;
- Be the first point of contact for the Information Commissioner and for individuals whose data is processed (employees, customers etc).
- Report to the highest relevant management level of the organisation – i.e., board level;
- Operate independently, and will not be dismissed or penalised for performing their task, however a DPO can still be dismissed or penalised for misconduct or negligence relating to their task; and
- Be provided adequate resources to enable DPOs to meet their obligations under UK GDPR or Part 3 of the Act.

5. Equality and Diversity

5.1 We are committed to fairness and equality for all regardless of colour, race, ethnicity, nationality, gender, sexual orientation, marital status, disability, age, religion or belief, family circumstances or offending history, as referred to in our relevant Group policies. Our aim is to ensure that our policies and procedures do not create an unfair disadvantage for anyone, either directly or indirectly.

6. Monitoring and Review

6.1 The next policy review is scheduled for April 2028 and then every two years thereafter.

6.2 We may update this policy from time to time to reflect changes in the law, regulations, or how we operate.

6.3 Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

6.4 The following performance standards, performance indicators and records will be maintained in pursuance of this Policy. Monitoring of Standards and KPIs is undertaken quarterly by Executive Risk Committee with an Annual Summary being reported to the Group Audit and Risk Committee.

Area	Standard/Record	PI
Subject Access Requests	Provide all disclosable personal information within one month	Number of SARs. Average number of calendar days Main Reasons for SARs
Data Breach identification and management	Clear outcome report with improvement plan and lessons learned logged for each reported breach	Number of reported breaches for year Main Reasons for Breaches ICO Notifications
Information Asset Register/Record of Processing Activities	Record of all significant Information Systems, Sharing Agreements and DPIAs held within the Group to be comprehensively recorded in a central database including owner, purpose, security measures and review date	N/A

Rolling programme of Data Audit Checks against Information Asset Register entries	Demonstrable Review Programme Clear outcome actions with improvement and mitigation actions plan and lessons learned logged for each audit	Number of completed IAR entry reviews in year % of Planned Review Programme Complete for the Year
ICO Registrations	Annual Registration for the Group, Platform Property Care and any other trading companies in the Group Record of Registrations, review date, fee paid on annual basis	100% Registrations
Data Protection Training	All Roles*: e-learning covering DPA (* except where limited access to personal data where self-study basic training materials will be used)	% of employees who have completed relevant DPA training in last 2 years

7. Associated Documents

7.1 List of documents - associated policies, procedures and publications:

- Data Protection Act 2018
- Data (Use and Access Act) 2025
- UK GDPR 2018
- Human Rights Act 1998
- Gender Recognition Act 2004
- Information Commissioner's Office - Code of Practice
- Regulatory Framework for Social Housing in England
- Acceptable Use Policy
- Bring Your Own Device (BYOD) Policy
- Clear Desk and Screen Policy
- Data Retention Policy and Schedule
- Disciplinary Policy and Procedure
- Information Security Policy
- Platform Housing Group Privacy Notice
- Platform Marketing Guidance

Author:	James Marsden
Document type:	Policy
Version 3:	Final
Version 3 **Approved by:** **Approved date:** **Release date:**	 Executive Team 20/05/2026 27/05/2026
Version 2 **Approved by:** **Approved date:** **Release date:**	 Executive Risk Committee 08/05/2024 08/05/2024
Customer Voice Panel:	No
Next review date:	05/2028
DPIA completed:	No
EIA completed:	Yes

Appendix 1

Data Protection Policy

Glossary of Terms and Definitions

A glossary of terms is listed below to assist with understanding of some of the terminology of the policy and legislation.

Term	Definition
Consent	This means consent of the data subject that is freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Data	Any recorded information held by the Group and from which a living individual can be identified, be this on paper or electronically.
Data Controller	A natural or legal person (in our case the Group) registered with the Information Commissioner's Office who determines the purposes and means of the processing of personal data.
Data Processor	A natural or legal person, public authority, agency or any other body that processes personal data on behalf of the Data Controller. Examples of this would be third-party contractors such as Amica 24.
Data Protection Officer	The appointed officer whose role in the organisation is to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.
Data Subject	A living individual who is the subject of the personal data/information. Examples would be current and former customers and employees.
Data Protection Act 2018	The General Data Protection Regulation forms part of the data protection regime in the UK, together with the Data Protection Act 2018.

Data (Use and Access) Act 2025	The Data (Use and Access) Act 2025 is UK legislation that updates and simplifies aspects of data protection law to enable more effective, responsible data use and data sharing, while maintaining high standards of privacy and protection for personal information.
Information Commissioner's Office (ICO)	The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. They are the Supervisory Authority (SA) for the UK.
Personal Data	Personal data only includes information relating to natural persons who: • can be identified or who are identifiable, directly from the information in question; or • can be indirectly identified from that information in combination with other information. Examples would include name, address, contact details, IP address plus any other information related to the individual.
Privacy and Electrical Communications Regulations (PECR)	These sit alongside the DPA and give people specific privacy rights in relation to electronic communications. There are specific rules on marketing calls, emails, texts, faxes and cookies (and similar technologies).
Processing	Any activity/operation performed on personal data, whether held electronically or manually, such as obtaining, recording, holding, disseminating, or making available the data, or carrying out any operation on the data. This includes, organising, adapting, amending and processing the data, retrieval, consultation, disclosure, erasure or destruction of the data. It is difficult to envisage any activity which does not amount to processing.
Special Category Data	More sensitive information relating to an individual's race/ethnic origin, political opinions/affiliations, religious beliefs, trade union membership, genetic data, health related, sexual life, and biometrics.