POL010
Data Protection Policy

Author:	Sarah Critchley
Owner:	Information Governance and IT Compliance Manager
Version Number:	v3.1
Date of Issue:	07/07/2020

CIRCULATION LIST

For Consultation
ITM&G EMT
SIRO
LJNCC/HR POLICY WORKING GROUP

RELATED DOCUMENTATION

Title
POL011 Records Management Policy
POL012 Freedom of Information Policy
Email Encryption Process
Privacy Policy – HR & Payroll Services
DPIA Process
Records in transit guidance
IT Acceptable Usage Policy
Data Subject request process
Personal data breach reporting process
Service specific privacy notice guidance

VERSION CONTROL

Version	Date	Author	Comments
2.01	20/07/2012	Sarah Slater	Review and update from November 2009 Policy V2.0
2.02	06/08/2012	Sarah Slater	Updated following SIRO Review
2.2	06/08/2012	Sarah Slater	Finalised for publication
2.21	02/10/2014	Sarah Slater	Policy Review
2.21	19/11/2014	Shane Agnew	Approved for publication
2.3	06/03/2015	Chris Daniels	Policy refresh approved by SA.
2.4	19/04/2016	Sarah Slater	Policy review no changes
2.5	01/02/2017	Sarah Critchley	Policy review, updated training repository details
3.0	08/03/2018	Sarah Critchley	GDPR and DPA2018 Refresh
3.1	07/07/2020	Lee Gardiner	Policy review, no changes

Document Distribution	All Councillors, Committees, Departments, Partners, and Employees of the Council, contractual third parties and agents of the Council who process, have access to, or custody of, Blackburn with Darwen Council information
Policy Review Date	July 2022

Contents

1 Introduction

This Policy replaces the previous Data Protection Policy V3.0 for Blackburn with Darwen Borough Council (The Council), dated March 2018.

Personal information is defined and regulated by the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (The Act). In addition Article 8 of the Human Rights Act 1998 gives broader protection by affording everyone the right to respect for their private and family life, home and correspondence.

Personal information is information about living, identifiable people. The definition includes - but is not limited to - information about their activities, opinions, lifestyle, background, character and choices.

The Council, as a Data Controller, is responsible for ensuring compliance with the data protection requirements outlined in this policy. Any breach of this policy will be taken seriously and may result in disciplinary action.

2 Scope

This policy relates to all instances where a data subject's personal data is processed relating to our citizens, service users, suppliers and other individuals, for a variety of purposes.

Everyone who works for The Council uses personal information. This policy ensures that all personal information that The Council obtains, uses or shares in its work is treated with care and respect, and is used lawfully and fairly.

Within this policy we will set out how we seek to protect personal data and ensure that employees understand the rules governing their use of personal data to which they have access in the course of their work.

This policy applies to all Elected Members, Committees, Departments, Partners, Volunteers, Employees of the Council, contracted third parties and agents of the Council (collectively referred to as 'users') who process, have access to, or custody of, Blackburn with Darwen Council information.

All users **must** understand and adhere to this policy and are responsible for ensuring the safety of all information controlled by the Council.

All users have a role to play and a contribution to make to the safe and secure use of the information that they hold.

The protection of personal data belonging to Council employees is not within the scope of this policy. This is covered in The Councils Recruitment & Employment Privacy Notice, within the **Privacy Policy** on the Corporate Website.

3 Definition

The General Data Protection Regulations (GDPR) are based on 6 principles that explain how personal information should be used. Compliance with these principles will ensure that information is secure, managed well, accurate and available.

Personal information can be obtained, used, shared and kept to provide services, look after people's interests and support the Council's objectives.

Data Protection supports efficient working and reinforces the Council's objective to provide appropriate and personalised services.
This policy sets out how the GDPR and the Data Protection Act 2018 applies to the Council, and sets out some specific measures to assist compliance.

The six Data Protection Principles can be found under Article 5 of the GDPR and are listed (a) to (f) as follows:

Article 5 – Principles relating to processing of personal data

1. Personal data shall be:

   (a) Processed lawfully, fairly and in a transparent manner
   (b) Collected for specified, explicit and legitimate purposes
   (c) Adequate, relevant and limited to what is necessary
   (d) Accurate and where necessary kept up to date
   (e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed
   (f) Processed in a manner that ensures appropriate security of the personal data

The Council is committed to ensuring that all processing of personal information complies with these principles.

A list of definitions for this policy have been made available at Appendix A.

4 Governance

4.1 The Data Protection Officer (DPO)

Under the GDPR it is mandatory for Local Authorities to designate a Data Protection Officer (DPO). This designation demonstrates a commitment to Data Protection and enhances the effectiveness of The Council's compliance efforts. The DPO is suitably qualified and has the necessary authority to provide guidance on all aspects of Data Protection. The DPO also has direct access to board level Directors.

The DPO's duties include:

- Ensuring the alignment of this Policy with Data Protection Regulations.
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs).
- Acting as a point of contact for and co-operating with Data Protection Authorities.
- Determining the need for notification to the Data Protection Authorities as a result of the Council's current or intended personal data processing activities.
- The operation of providing prompt and appropriate responses to Data Subject requests.
- Informing senior managers, officers and directors of any potential corporate, civil and criminal penalties which may be levied against the Council and/or its employees for a violation of applicable data protection laws.
- Ensuring establishment procedures and standard contractual provisions for obtaining compliance with this policy by any third party who;
  - Provides personal data to The Council
  - Receives personal data from The Council
  - Has access to personal data collected or processed by The Council

The DPO for Blackburn with Darwen Council is
sarah.critchley@blackburn.gov.uk
01254 585226.
Supported by the Information Governance team accesstoinformation@blackburn.gov.uk

5 Data Protection by Design

5.1 Data Protection Impact Assessments (DPIAs)

To ensure that all Data Protection requirements are identified and addressed, when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each requirement must go through an approval process before continuing.

The Council must ensure that a Data Protection Impact Assessment (DPIA) is conducted in co-operation with the DPO, for all new/revised systems or processes for which it has responsibility.

The subsequent findings of the DPIA must then be submitted to the Senior Information Risk Officer (SIRO) for review and approval.

The **Data Protection Impact Assessment Procedural guide** can be found on the Council's Information Governance intranet page.

6 Compliance Monitoring

6.1 Data Protection Compliance Audit

To confirm that an adequate level of compliance is being achieved by all users in relation to this Policy, the DPO will initiate routine Data Protection compliance audits to assess:

- Compliance with the policy in relation to the protection of personal data including assignment of responsibilities and training of employees.
- The effectiveness of data protection related operational practices.
- The level of understanding of data protection policies and privacy notices.
- The accuracy of personal data being stored.
- The adequacy of procedures for redressing poor compliance and personal data breaches.

7 Data Collection

7.1 Data sources

Personal data should only be collected directly from the Data Subject, unless one of the following applies:

- The nature of the business purpose necessitates collection of personal data from other bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject.

If personal data is collected from someone other than the data subject then the data subject should be informed **unless** one of the following applies:

- The Data Subject has received the required information by other means.
- The Information must remain confidential due to a professional secrecy obligation.

Where it is determined that notification to a data subject is required, this must be carried out no later than one month from the first collection or recording of the personal data.

7.2 Data Subject Consent

The Council will obtain personal data only by lawful and fair means and where appropriate, with the knowledge of the individual concerned.

Where a need exists to request and receive consent of an individual prior to the collection, use or disclosure of personal data, the Council is committed to seeking such consent.

In all cases consent must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of

personal data relating to him or her. This can be obtained by a written statement, including by electronic means, or an oral statement.

The process for obtaining consent therefore, must include provision for:

- Ensuring the request for consent is presented in a manner clearly distinguishable from other matters.
- Ensuring the request for consent is made in an intelligible and easily accessible form using plain language.
- Ensuring consent is freely given (ie not based on a contract this is conditional to the processing of personal data).
- Documenting the date, method, validity and content of the consent.
- Providing a simple method for the data subject to be able to withdraw consent at any time.

Once consent is withdrawn by the data subject, The Council must cease processing data for the specified purpose without undue delay.

7.3 Privacy Notices

The Council will provide data subjects with information as to the purpose of the processing of their Personal Data by way of a Privacy Notice.

Where any personal data is collected from the data subject, including where a data subject is asked to give consent to the processing of personal data, The Council will direct the data subject to a transparent Privacy Notices that details the following:

- Who you are
- What you are going to do with their information
- Who you will share their information with
- How long you expect to keep their information
- Contact details of the DPO

The Council will host a **Primary Privacy Notice** on the corporate website. This notice explains who we are, how we use personal information, advises about individuals privacy rights and how the law protects them.

All service area's that collect personal data must develop a service specific privacy notice relevant to their data processing activities. A Service Specific Privacy Notice guidance document is hosted on the **Privacy Notices** section of the Information Governance intranet page.

All service specific privacy notices must be approved by the DPO prior to publication on The Council's corporate website.

7.4 Records of Processing Activity (ROPA) register

The Council will maintain a Records of Processing Activity register. Each record will contain (at least) the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed
- where applicable, transfers of personal data to a third country or an international organisation, including documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures

Keeping a record of The Council's processing activities is not a one-off exercise. The information documented must reflect the current situation as regards the processing of personal data. These records should be regarded as a living document to be updated as and when necessary.

Regular reviews of the personal data processing will be undertaken by the DPO to ensure all processing records remain accurate and up to date.

It is the responsibility of each Information Asset owner to ensure that this register is continually monitored for accuracy.

7.5 Data Processing

7.5.1 Processing Personal Data

The Council will process personal data in accordance with all applicable laws and contractual obligations. More specifically, The Council will not process personal data unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract, or prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the data controller is subject.
- Processing is necessary in order to protect he vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

There are some circumstances where personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. Please seek advice from your DPO before any such processing commences.

Prior approval must be obtained from the DPO using the **Data Protection Impact Assessment Procedural guide** when implementing new processes and the basis for the processing must be clearly recorded on The Council's Record of Processing Activity register.

7.5.2 Processing Special Categories of Data

The Council will only process special categories of data (also known as sensitive data) where the data subject explicitly consents to such processing, or where one of the following applies:

- The processing is specifically authorised or required by law.
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- The processing relates to personal data which has already been made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is necessary for reasons of substantial public interest.
- Further conditions include limitations based upon national law related to the processing of genetic data, biometric data or data concerning health and for reasons of public interest in the area of public health.

Processing of personal data relating to criminal convictions and offences will only be carried out under the control of the official authority.

In each case, prior approval must be obtained from the DPO using the Data Protection Impact Assessment template contained within the **Data Protection Impact Assessment Procedural guide** and the basis for the processing must be clearly recorded on The Council's Record of Processing Activity register.

7.5.3 Children's Data

Children under the age of 13 are unable to consent to the processing of personal data for information society services, which is any service normally provided at a distance, by electronic means and at the individual request of a recipient of services. Consent must therefore, be sought from the person who holds parental responsibility over the child.

Where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

Should The Council foresee a business need for obtaining parental consent for information society services offered directly to a child, guidance and approval must be obtained from the DPO before the processing of a child's personal data may commence.

7.5.4 Data Quality

The Council will adopt all necessary measures to ensure that the personal data it collects and processes is complete and accurate. Measures to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any data protection principles.
- Restriction rather than deletion relating to:
    - Law prohibiting erasure.
    - Erasure impairing legitimate interests of data subject.
    - The data subject disputing that the personal data is correct and it cannot be ascertained otherwise.

7.5.5 Profiling & Automated decision making

The Council will only engage in profiling and automated decision making where it is necessary to enter into/to perform, a contract with the data subject, or where it is authorised by the law. In such cases the data subject will be given the opportunity to:

- Express their point of view
- Obtain an explanation for the automated decision
- Review the logic used by the automated system
- Supplement the automated system with additional data
- Have a human carry out a review of the automated decision
- Contest the automated decision
- Object to the automated decision-making being carried out.

7.5.6 Digital marketing

The Council will not send promotional or direct marketing material through digital channels such as mobile phones, email and internet without first obtaining explicit consent from the data subject.

Where personal data processing is approved for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to withdraw their consent to having their data processed for such purposes at any stage.

Once an objection to digital marketing is received The Council must cease processing data for this purpose without undue delay.

7.6 Data Retention

7.6.1 Records Management

Departments must put in place adequate records management procedures, including measures to ensure that working records about people are fair, accurate, up-to-date and not excessive.

Records about people must be secure, traceable and accounted for at all times and be disposed of securely in accordance with the appropriate disposal schedule found within the **Records Management Policy**

Records management procedures, including retention and disposal, apply equally to paper and electronic records including emails.

Departments will regularly need to assure themselves that they are compliant with statute by reporting any discrepancies.

The length of time for which The Council needs to retain personal data is set out in the Corporate '**Retention Schedule'** All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

7.6.2 Archiving

The Council has an Email Retention Policy which determines the email archiving process and retention period.

The Council also has an existing process that manages off-site archiving of hardy copy documentation. This process includes archiving, storage, recall and destruction in-line with pre-agreed destruction dates. For information relating to this process please contact the CAPS team

All users are responsible for ensuring that personal data records that are required to be kept for archiving purposes are managed in line with the **Records Management Policy**

7.7 Awareness and Training

All users will participate in an on-going programme of data protection training, provided by Information Governance. **All users are required to complete the Corporate Information Governance Training prior to accessing any personal information on Council systems**. The annual completion of this training is mandatory. The training content is located on the **Me Learning platform**. Compliance checks will be made on a quarterly basis to ensure all users are up to date.

7.8 Information Security

7.8.1 Physical Security and Breach Reporting

All premises and electronic systems where personal information is held must have adequate security. Access to areas where information is held must be controlled, paper files containing personal information must be locked away when not in use, and computer data must be protected adequately.

Care must always be taken if personal information recorded on paper is used outside council premises, in accordance with the Council's **Paper Records Secure Handling in Transit Policy**. Personal information must only be stored on devices or equipment that are encrypted, under the Council's control and which have been approved for use by the ITM&G Department.

Access to information must be restricted to authorised employees only; such employees must receive training on the security of the system prior to being given access to it.

Electronic data must only ever be stored on official Council servers.

All users must adhere to **The Councils IT Acceptable Use Policy**. This Policy outlines the standards of conduct that are required of you when using all electronic communications and systems.

The Information Governance section must be notified of any actual loss, theft or accidental disclosure of personal information.

Any individual who suspects that a personal data breach has occurred due to theft or exposure of personal data must immediately notify the DPO.

The DPO will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the DPO will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved. For significant personal data breaches, The DPO will initiate an emergency response team to co-ordinate and manage the personal data breach response.

To establish what you need to do in the event of a personal data breach, please refer to the **Data Protection Impact Assessment Procedural guide** on The Council intranet page.

7.8.2 The Need to know

Access to personal information must only be given to those who need it. Personal information should only be used when necessary and not purely because it is convenient to do so.

Each Information Asset Owner is responsible for restricting access to personal information and ensuring compliance with this policy.

All access to systems containing personal information for maintenance or testing must be logged. Where a system has the facility to log the creation of users, and the accesses those users have made, this facility must be switched on.

7.8.3 Complaints handling

Data subjects with a complaint about the processing of their personal data are required to put forward the matter in writing to the DPO. An investigation of the complaint will be carried out to the extent that it is appropriate based on the merits of the specific case. The DPO will inform the data subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the data subject and the DPO, then the data subject may, at their option, seek redress through the Data Protection Authority (The Information Commissioner) within the applicable jurisdiction.

7.9 Data Subject Requests

The DPO is responsible for enabling and facilitating the exercise of data subject rights related to:

- Information access
- Objection to processing
- Objection to automated decision-making and profiling
- Restriction of processing
- Data portability
- Data rectification
- Data erasure

If an individual makes a request relating to any of the rights listed above, the DPO will consider each request in accordance with all applicable data protection laws and regulations.

No administration fee will be charged for complying with such a request unless the request is deemed to be unnecessary, excessive in nature, or a repeated request.

All subject access requests must be answered within 1 month following the date of receipt. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. The Controller however, must notify the data subject of any such extension within one month of receipt of the request together with the reasons for the delay.

All requests received for access to, or deletion/rectification of personal data must be directed to the DPO via **accesstoinformation@blackburn.gov.uk**.

Alternatively you could guide the data subject to the **'How to request your personal information'** form on the Council Internet page.

7.10 Information Sharing Agreements

An Information Sharing Agreement or protocol is not a legal requirement to share information. Sharing can happen without one. An agreement does not create a legal gateway if one does not already exist however, the use of a protocol will ensure best practice by all partners in any information sharing partnership.

All agreements or protocols between the Council and outside agencies must be registered with the Information Governance Section and agreed with the Senior Information Risk Officer (SIRO) and the DPO.

Departments must not sign any agreement without seeking advice from the DPO. Agreements should be drawn up after consultation between organisations, not imposed by one on another.

Information Governance must be consulted whenever a Department wishes to share information with either internal or external partners. For guidance on best practice data sharing, please refer to the **Sharing Personal Data guidance** on the Council's intranet page

7.11 Security of Transfer

7.11.1 Security of Transfer to Third Party Data Controllers and Data Processors

The Council will only transfer personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where third party processing takes place, The Council will first identify if the third party is considered a data controller or a data processor of the data being transferred.

Where the third party is deemed to be a data controller, The Council will, with assistance from the DPO, enter into an appropriate agreement with the controller to clarify each party's responsibilities in respect of the personal data transferred.

Where the third party is deemed to be a data processor, The Council will, with assistance from the DPO, enter into an adequate processing agreement with the processor to protect the personal data from further disclosure and to only allow processing in compliance with The Council's instructions.

The DPO will ensure that all transfers of data comply with appropriate technical and organisational measures to protect the personal data.

The Council will also ensure that all third parties are issued with the procedures for notification of personal data breaches.

7.11.2 Security of personal information disclosures.

When sending personal information outside the Council, users must take steps to ensure that only appropriate people will see it.

If email is considered to be the best option, employees must use the correct email address and be aware that email inboxes may be monitored by managers or others who may not be entitled to access personal information.

Personal information must only be shared by secure transfer. This will mean using a GC email system for electronic transfers of personal information to other Government Agencies. Access to GC Mail is carried out by an authorised process. To apply for a GC Mail account, please refer to the **GCSX Mail request process** on the Council's intranet page.

Should the recipient not have access to the GC email system, all Council users have access to the corporate **email encryption service** which enables the secure transfer of personal and sensitive information to non GC mail users.

7.12 Contracts

All contracts should include measures to ensure that the Council's data is used safely and appropriately.

Information supplied to 3rd Party contractors must only be used for agreed purposes, and must not be used or disclosed for any other reason without consent from the Information Asset Owner.

Due diligence must be carried out in relation to all contracts or agreements that involve the sharing of personal information. Risk assessments are required to assess the organisational maturity of a 3rd party's data protection processes. All contractors that are to have access to the Council's information will be required to provide evidence that data protection training has been completed.

7.13 Confidentiality

Information explicitly accepted in confidence or as part of a confidential relationship can only be disclosed to someone else in exceptional circumstances.

Employees must not disclose confidential information to anyone else without the permission of the individual who first gave the information to them, unless the information is about serious wrong-doing or harm.

All employees have a duty to report any criminal activity or wrong doing to the proper authorities.

The Council operates a Whistleblowing Policy, which provides further advice on what to do in these situations. This Policy is on the Council's intranet.

7.14 Testing and Training

When developing or testing any new system or process, or working on an existing system for the purpose of testing or training, information about real people must not be used. This applies equally to users and 3rd parties when testing or upgrading systems. Personal information must not be used in any training exercise – real examples must be fictionalised to the point where a person cannot be identified.

8 Policy Compliance

The Council will ensure that users are aware of their responsibility for processing personal data along with the contents of this policy. In addition The Council will make sure that all third parties

engaged to process personal data on their behalf are aware of and comply with the contents of this policy. Assurance of such compliance will be obtained from all third parties prior to granting them access to personal data controlled by The Council.

The Audit and Assurance section will periodically audit departments using the Information Commissioner's audit guidance to ensure that all parts of The Council comply with the current UK Data Protection Legislation.

If any user is found to have breached this policy, they will be subject to Blackburn with Darwen Council disciplinary procedure. If a criminal offence is considered to have been committed further action will be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the DPO.

9 Policy Governance

The following table identifies who within Blackburn with Darwen Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Director of Digital and Business Change
Accountable	SIRO
Consulted	Policy Working Group/Unions/Exec Board
Informed	All Council Employees, All Temporary Employees, All Contractors, all 3rd Party Contract Holders, all Volunteers.

10 Review and Revision

This policy will be reviewed every two years to ensure that it takes account of new legislation and expected developments in the areas of personal privacy and public sector information sharing.

Policy review will be undertaken by the Information Governance Team.

Appendix A

Definitions:

Employee
An individual who works part-time or full time for The Council under a contract of employment, whether oral or written, express or implied and has recognised duties. Includes temporary employees.

Users
Elected Members, Committees, Departments, Partners, Volunteers, Employees of the Council, contracted third parties and agents of the Council (collectively referred to as 'users') who process, have access to, or custody of Council information.

Third Party
An external organisation with which The Council conducts business under the direct authority of The Council, processing the personal data of Council service users.

Personal Data
Any information (including opinions and intentions) which relates to an identified or identifiable natural person.

Identifiable natural person
Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Controller
A natural or legal person, public authority agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Subject
The identified or identifiable natural person to which the data refers

Process, Processed, Processing
Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptations or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Consent
Any freely given, specific informed and unambiguous indication of the data subjects wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Special categories of data
Personal data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Profiling
Any form of automated processing of personal data where personal data is used to evaluate specific or general characteristics relating to an identifiable natural person. In particular to analyse or predict certain aspects concerning that natural persons performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.
Personal data breach

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.

Encryption
The process of converting information or data into code, to prevent unauthorised access.