Glossary of commonly used Data Protection Terms

For the Adoption Authority of Ireland

ÚDARÁS UCHTÁLA na hÉIREANN
THE ADOPTION AUTHORITY of IRELAND

Revision and Approval History					
Version	**Revised By**	**Revision Date**	**Approved By**	**Approval Date**	**Comments**
1.0	Mathesons	23/10/2020			
Reviewed	**DPO**	**24/08/2021**			

Within the Adoption Authority we often use terms in relation Data Protection and GDPR.
Here is a list of the most common data privacy terms everyone should be aware of
These definitions of terms are encountered most often in the official policy documents of the Adoption Authority of Ireland (the "**Adoption Authority**") are provided below to ensure clarity to the reader.

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

Examples of personal data include:

- Name
- Address
- Date of Birth
- Phone number
- Email address
- Employee number

"**Accountability**" – The controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. The measures implemented shall be reviewed and updated where necessary. ("**Accountability Principle**");

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

"**Data**" means Personal Data unless otherwise defined or explained;

"Data Protection" refers to any software or activity related to protecting the safety and integrity of private data.

The **DC** "**Data Controller**" or "**Controller**" is the natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data; the Adoption Authority acts as a Data Controller.

"**Data Protection Stakeholders**" means the Board of the Adoption Authority and the Senior Management Team and the Data Protection Officer.

Data Protection (DP) Principles
As set out by the GDPR, Data Protection Principles pertain to the state of personal data in relation to processing, collection, status, storage, compliance and responsibility.

"**DPA 2018**": means the Data Protection Act 2018;

"**Filing System**" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Counsel, commonly known as the General Data Protection Regulation; The General Data Protection Regulation (GDPR) is a European data privacy law that extends to all businesses (including businesses that operate outside of Europe) that offer goods and services to European residents and collect personal data in the process.

A "**Personal data breach**" is 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. This includes breaches that are the result of both accidental and deliberate actions.

Breach Disclosure
The process of notifying regulators and/or victims of incidents affecting the confidentiality and security of their personal data.

The **DP**/ "**Processor**" is a natural or legal person, public authority, agency or any other body, which processes personal data on behalf of a Data Controller;

"**Processing**" is defined as any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The "**Processing Purpose**" is the pre-defined reason for collecting and processing a specific set of data e.g. to set up a customer account, to complete a sale, or to market goods or services. Each purpose should be paired with a description of data use. All pre-defined purposes should be listed in a privacy notice made available to data subjects before data is collected, and a data protection impact assessment should include a check to ensure pre-defined purposes do not differ from current data uses;

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

"**Special categories of personal data**" (sometimes referred to as "**sensitive personal data**") are types of personal data which are subject to stricter processing requirements. This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely

identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

"**Supervisory Authority**" – is the independent public authority with responsibility for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of the natural persons in relation to processing and to facilitate the free flow of personal data within the European Union. In the context of the Irish Jurisdiction, this authority is vested in the office of the Irish Data Protection Commission. See **DPC** below.

SAR A Subject Access Request- This is a request made by an individual who wants to see a copy of the information an organisation holds about them.

Authentication/Verification Authentication is the process of verifying a person's identity before granting access to a resource.

Consent The right of a data subject to decline or agree to the collection and processing of their personal data.

Anonymization Also known as Data Masking, this is the process of altering personally identifiable data so that it cannot be used to identify an individual.

Pseudonymisation with pseudonymisation the individual can still be identified – e.g. at its most basic level changing an employee's name to an identification number instead and removing all of their other personal details is pseudonymisation.

RTBF/RTE ***Right to be forgotten /Right to Erasure: creates the right of a data subject*** **"**to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay**".**
This is an individual's right to have their personal data deleted by a business or other organization possessing that data.

Data Portability A right under the GDPR that ensures data subjects are allowed to receive their personal data from a data controller in a commonly used and machine-readable format.

Sensitive Data Sensitive data is a type of data that describes a person and that used together to identify that person. This includes personal information about an individual's race, ethnic origin, marital status, age, colour, and religious, philosophical, health or political affiliations.

Encryption Encryption is a type of data protection that transforms plaintext data into cipher text, effectively hiding the original data's meaning. Encryption renders information unreadable without an encryption key.

Human error/"Near misses" Human error is the cause of most internal breaches in the Adoption Authority and other organisations– simply not being aware that a certain activity poses a risk. Examples of human error include accidentally introducing Malware through a device or phishing email, having a weak or easily discovered password, a shared password, or accidentally sharing sensitive information with someone outside the Adoption Authority.

Ransomware Malware that encrypts a device and denies the user access to key files unless they pay a fee to recover them i.e. a type of blackmail.

Malware Used to describe malicious software intended to infiltrate computers or computer networks.

Hacker A hacker is an individual that violates computer security through technological means.

Cookie A small file stored by a website that tracks browser activity, remembers user preferences and keeps users logged in for subsequent sessions.

Commonly used abbreviations

DPO	Data Protection Officer
DPC	Data Protection Commissioner (IRL) A Data Protection Authority (DPA) is an independent public authority that supervises and enforces data protection laws.
ICO	Information Commissioners Office (UK) as above, in UK
DP	Data Processor
DS	Data Subject
EEA	European Economic Area
DPIA	Data Protection Impact Assessment -The process by which risks are identified and the impact of those risks is determined.
PIA	Privacy Impact Assessment.