Commonly Asked Questions about the Basics of Data Protection

An Coimisiún um Chosaint Sonraí
Data Protection Commission

DATA PROTECTION BASICS

When does data protection law apply and what does it cover?

- Data protection law covers most situations in which information about somebody (the **'personal data'** of a **'data subject'**) is used in some way (**'processed'**) by some other person or organisation (the **'controller'**), other than in a purely personal context.
- The Data Protection Commission (**DPC**) is responsible for regulating different sets of laws, which cover different ways and circumstances in which personal data might be processed. These laws are set out below and on the DPC's website.
- The 'General Data Protection Regulation' (**GDPR**) is the law which applies to most kinds of processing of personal data and it applies directly in Ireland (and across the EU), along with further national rules set out in the Irish **Data Protection Act 2018**.
- However, the GDPR does *not* apply to the processing of personal data by an individual for **'purely personal or household'** activities, with no connection to a professional or commercial activity. This is sometimes known as the 'personal/household/domestic exemption'. This might cover activities such as correspondence, keeping an address book, or certain social networking, where these activities are purely personal. The GDPR would still apply to controllers who process personal data to facilitate these activities (such as a social network).
- Where processing takes place for **law enforcement purposes** (such as preventing or detecting crime) the GDPR does not apply, and instead the 'Law Enforcement Directive' (**LED**) covers these situations, the rules for which are found mainly in Part 5 of the Data Protection Act 2018 (which implements the LED into Irish law).
- Ireland's '**ePrivacy Regulations**' (S.I. 336/2011, which implemented the EU 'ePrivacy Directive') are an extra set of rules which apply to certain types of processing, including **electronic direct marketing** and **cookies**, and these rules apply in addition to the rules found in the Data Protection Act 2018 and the GDPR.
- These laws set out various obligations on data controllers and rights for data subjects, some of which are discussed below. They also set out the powers and responsibilities of the DPC. If you have a concern that a controller has failed to follow the law or uphold your rights, the guidance below should help you **(a)** make a **request** to a controller, or **(b)** make a **complaint** to the DPC, if they fail to comply with your request or their obligations under data protection law.

What are 'personal data' and when are they 'processed'?

- Personal data basically means any information **about a living person**, where that person either is **identified or could be identified**. Personal data can cover various types of information, such as name, date of birth, email address, phone number, address, physical characteristics, or location data – once it is clear to whom that information relates, or it is reasonably possible to find out.
- Personal data doesn't have to be in **written form**, it can also be information about what a data subject looks or sounds like, for example **photos** or **audio** or **video** recordings, but data protection law only applies where that information is processed by **'automated means'** (such as electronically) or as part of some other sort of **filing system**.
- Personal data can be information where the data subject is **identified** – "*John's favourite colour is blue*" – or where they are **'identifiable'** – "*John's sister's favourite colour is blue*" (where you don't know his sister's identity, but could find out using context and/or additional information).
- Even where personal information is partially anonymised, or **'pseudonymised'**, but this could be reversed and the data subject could possibly be identified using additional information, it should **still be considered personal data**. However, if information is truly anonymised, irreversibly, and could not be traced back to an identified person, it is not considered personal data.
- To determine whether a person is 'identifiable', particularly where the information about that person is pseudonymised, all the **methods and information reasonably likely** to be used by the controller or other person **to identify** someone, either directly or indirectly, have to be considered.
- Certain types of **sensitive** personal data, called **'special categories'**, are subject to additional protection under the GDPR, and their processing is generally prohibited, except for where specific requirements are met (such as having explicit consent), as set out in detail in **Article 9 GDPR**. The special categories are: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data processed to uniquely identify a person; data concerning health; and data concerning a person's sex life or sexual orientation.
- Data protection law governs situations where personal data are **'processed'**. Processing basically means **using personal data in *any* way**, including; collecting, storing, retrieving, consulting, disclosing or sharing with someone else, erasing, or destroying personal data. Although, as mentioned above, data protection law does not apply where this is done for purely personal or household activities.

What is a data 'controller' and what are their obligations?

- A '**controller**' refers to a person, company, or other body that **decides how and why** a data subject's personal data are processed. If two or more persons or entities decide how and why personal data are processed, they may be **'joint controllers'**, and they would both **share responsibility** for the data processing obligations.
- A **'processor**' refers to a person, company, or other body which processes personal data **on behalf of a controller**. They don't decide how or why processing takes place, but instead carry out processing on the orders of a controller.
- As mentioned above, if a person (but not a company or other body) decides how and why personal data are processed, and/or processes that data, but they only do so in a **purely personal or household capacity**, they will not be subject to the obligations of controllers under the GDPR or Data Protection Act 2018.
- Regarding processing for the **purposes of law enforcement**, the specific rules in the LED and Part 5 of the Data Protection Act only apply to processing where the controller is a **'competent authority'**. This is defined as a **public authority** which is 'competent' for law enforcement purposes (such as the Gardaí or the Revenue Commissioners), or any **other body which is authorised by law** to exercise public authority and powers for law enforcement purposes.
- Controllers have a **range of obligations** under data protection law, and in particular must comply with the **principles of data protection**, as found in **Article 5 GDPR**, ensuring personal data are: processed lawfully, fairly and transparently; processed for specific purposes; limited to what is necessary; kept accurate and up to date; stored for no longer than necessary; and protected against unauthorised or unlawful processing, accidental loss, destruction, or damage. Controllers must also be able to **demonstrate compliance** with these principles, under the principle of accountability.
- Under the principle of **transparency**, controllers should **provide certain information** to data subjects when they collect their personal data, such as: the identity of the controller; the contact details of the controller and (if they have one) their 'data protection officer' (DPO); the purposes and 'legal basis' for the processing; who the data will be shared with; how long the data will be stored; and the existence of the data subject's various rights.
- If you want to exercise any of your rights as a data subject, the first step is to **identify** who the **data controller** is, and then to make your **data subject request** to them (more information on data subject rights and requests can be found below). If they don't respond or don't allow you to exercise your rights, or if you think there has been any other infringement of data protection law, you can contact the DPC.

What is meant by the 'legal basis' for processing personal data?

- In data protection terms a 'legal basis' (also referred to as a 'lawful basis' or 'lawful reason') means the **legal justification for the processing** of personal data. A valid legal basis is required in all cases if a data subject's personal data are to be lawfully processed in line with data protection law.
- Under the GDPR, there are **six possible legal bases** for processing personal data, found in Article 6, namely: consent; contractual necessity; compliance with a legal obligation; protecting vital interests; performance of an official or public task; and legitimate interests (where the interest is not outweighed by the data subject's).
- There is **no hierarchy or preferred option** within this list, but instead all processing of personal data should be based on the **legal basis which is most appropriate** in the specific circumstances of that processing. Controllers should be aware that there may be different legal bases applicable to different types of processing of the same personal data.
- It is important to note that **'consent'**, whilst perhaps the most well-known, is **not the only legal basis for processing** personal data – or even the most appropriate in many cases. Where consent is used, there are a number of **special requirements** for it to provide a valid legal basis for processing; it has to be specific, informed, and unambiguous, and it has to be freely given. It must always be **possible to withdraw** consent after it has been granted; once it is withdrawn, the personal data cannot be processed any further on the basis of consent.
- As mentioned above, under the GDPR, certain **special categories** of personal data should not be processed except in **limited circumstances**. Such processing requires both a legal basis under Article 6 GDPR, as well as meeting one of the exceptions in Article 9 (such as explicit consent or protection of vital interests) which allow such data to be processed.
- It is the **responsibility of every controller to identify** which legal basis they are relying on for each type of processing of personal data they engage in. This information should be **provided to data subjects**, as part of the principle of transparency, and controllers should always be able to identify the legal basis they are relying on for processing **if asked by a data subject or the DPC**.
- For controllers processing personal data for **law enforcement purposes** under the LED, the justification for such processing must either be that they have the **consent** of the data subject **or** that the processing is **necessary for the performance** of their **functions** for the purpose of 'the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against, and the prevention of, threats to public security', or 'the execution of criminal penalties'.

What rights have data subjects and how can they be exercised?

- Individuals have a **number of specific rights** under data protection law to keep them informed and in control of the processing of their personal data. The most commonly exercised of those rights are those found under the GDPR (in Articles 12-22 and 34).
- The **data subject rights** under the **GDPR** include: the right to be informed if, how, and why your data are being processed; the right to access and get a copy of your data; the right to have your data corrected or supplemented if it is inaccurate or incomplete; the right to have your data deleted or erased; the right to limit or restrict how your data are used; the right to data portability; the right to object to processing of your data; and the right not to be subject to automated decisions without human involvement, where it would significantly affect you.
- **Information provided** to data subjects when these rights are exercised must be **transparent, understandable and easily accessible**, using clear and plain language. The information should be provided in writing, or other means, including, where appropriate, electronically. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is clear or can be proven.
- It is important to note that these **rights are not absolute**, and are subject to a number of **limitations** and **restrictions**. Certain rights apply to all processing activities, such as the right to information or to access to personal data, whereas other rights only apply in certain circumstances, such as the rights to erasure, restriction, portability, and objection. Both the GDPR and the Data Protection Act 2018 set out limitations and restrictions on these rights.
- Where personal data are processed for law enforcement purposed under the **LED**, data subjects have **similar rights**, found in Sections 89-95 of the Data Protection Act 2018, which are subject to a range of restrictions. These rights include the right to information, right of access, and rights to rectification, erasure, and restriction.
- To exercise any of these data protection rights, data subjects should first make a **data subject request to the data controller**. If the controller does not respond or does not allow a data subject to exercise their rights, data subjects may then wish to contact the DPC to make a complaint.
- More information on the various data subject rights, their extent and limitations, and how to exercise them, can be found on the guidance for individuals on the DPC's website.

When can a data controller send electronic direct marketing?

- Electronic direct marketing involves the sending or making of **unsolicited marketing** communications, including by **email, text message, phone or fax,** to a recipient. These communications are usually made for the purpose of advertising a product or service or for other promotional purposes. Electronic direct marketing of this kind is subject to specific rules that are set out in the ePrivacy Regulations (S.I. 336/2011).
- Under the ePrivacy Regulations, the organisation or person on whose behalf direct marketing communications are sent must generally have obtained the **prior consent** of the **intended recipient**, agreeing to receive such communications – and they must be **able to demonstrate** that the recipient actively agreed in advance to receiving such communications. Consent must be a clear, affirmative act, freely given, specific, informed, and unambiguous, as required by the GDPR (these two laws work together in such cases). Where consent to marketing is given, it **can be withdrawn** at any time.
- The GDPR notes that **silence**, **pre-ticked boxes**, or **inactivity** will not generally be enough to signify consent. This means that a direct marketer cannot normally, for example, rely on the recipient failing to untick a pre-ticked box as a valid form of consent. Each direct marketing message sent by email or text should also **identify the sender**, or on whose behalf it is being sent, and **provide a valid address** so that the recipient may **request** that the sending of such **messages should cease.**
- There are certain **limited exceptions** where electronic direct marketing communications can be sent without obtaining the prior consent of the recipient. For example, controllers may send electronic direct marketing messages to their customers **without explicitly having consent**, but only if; they collected the contact details during the sale of a product or service; they're marketing their own product or service; it is a similar product or service to the original sale; the first marketing message was sent within 12 months of the original sale; and, most importantly, the data subject was given a **chance to object to receiving** marketing messages, both at the time of the original sale and with each subsequent marketing message.
- Under the GDPR (Article 21), individuals also have the **right to object at any time** to their personal data being used for direct marketing purposes. This includes not just electronic direct marketing but **also postal and other forms** of direct marketing. If such an objection is made, then the organisation **must cease** using their personal data for direct marketing; this includes **deleting** it from any **marketing databases**.
- More detailed information can be found on the DPC website on electronic direct marketing, including guidance the DPC has published on the national directory database (NDD) and the issuance of e-receipts.

What are the rules regarding the use of cookies on websites?

- A cookie is a small text file that can be placed and **stored on a user's computer or device** by a website the user has visited, and can serve a number of purposes. These include enabling the website to recognise the user the next time the user visits it and to **'remember' the user's actions** or **preferences** over a period of time, or the cookie may contain data related to the **function or delivery** of the website.
- Cookies can be set by the **owner of the website** or, in some cases, by **third party services**. In such a case, the website owner allows the third party to present other information, run **content** or **advertisements**, or provide other functionality such as **analytics**, through its website.
- The website owner, or third party services, must normally obtain consent from users to place and use cookies and other similar technologies on a user's computer or device, as required by the ePrivacy Regulations (S.I. 336/2011). However, the user's **consent is not required** where the cookie or other technology is **strictly necessary to provide** the user with the **service** they have requested – for example, cookies which may be needed to run certain essential functions on a website.
- The website owner must also provide users with certain **easily accessible**, **clear**, and **comprehensive information** on the type of cookies or similar technology they are using and the **purpose** for which they are using it.
- Further guidance on the use of cookies and other similar technologies can be found on the DPC website.