Frequently Asked Questions - FAQ

General

1.1 What is personal data?

This is a broad concept. More extensive guidance is available at the following link: What is Personal Data?

The definition in the Act reads:
"personal data" means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller."
It covers any information that relates to an identifiable, living individual. However, it needs to be borne in mind that data may become personal from information that could likely come into the possession of a data controller. Often a case by case assessment must be made taking account of some of the above considerations as to whether data could be deemed to be personal.

1**.2 What is a Data Controller?**

A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.

1**.3 What is meant by sensitive personal data?**

Sensitive personal data is defined in the Data Protection Acts as any personal data as to -
(a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
(b) whether the data subject is a member of a trade union
(c) the physical or mental health or condition or sexual life of the data subject,
(d) the commission or alleged commission of any offence by the data subject, or
(e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

The Data Protection Acts require additional conditions to be met for the processing of such data to be legitimate. Usually this will be the **explicit** consent of the person about whom the data relates.

1.4 What is excessive information?

The Data Protection Acts require that only the minimum necessary personal data should be sought and used to allow for the performance of the function to which it relates. This requires a Data Controller in all situations to be certain that the data that is being sought is appropriate to the reason for which it was sought. A data controller must be able to show that each piece of personal data sought from a person is needed for a legitimate reason. Where data is not needed for the reason for which it was sought this would constitute a breach of the Data Protection Acts.

1.5 Do the Acts apply to information kept by an individual in their personal capacity?

The processing of personal data kept by an individual and concerned solely with the management of his/her personal, family or household affairs or kept by an individual for recreational purposes is exempt from the provisions of the Acts. For example, this exemption would generally apply to the use of CCTV in a domestic environment.

1.6 What powers does the Data Protection Commissioner have?

The Data Protection Commissioner is responsible for ensuring that people's rights are respected, and that the persons who keep personal information meet their responsibilities. The Commissioner's approach to complaints, as provided under the Acts, is to try to reach an amicable resolution to the matter which is the subject of the complaint. In cases where it is not possible to reach an amicable resolution, a complainant may ask the Commissioner to make a formal decision as to whether a contravention has occurred. However, the Commissioner does not have the power to award compensation. The Commissioner's main priority, if he upholds your complaint, is that the data controller complies with the law and puts matters right. If the Commissioner rejects your complaint, he will inform you of this in writing. If you disagree with the Commissioner's finding, you have the right to appeal the decision to the Circuit Court.

The Data Protection Acts makes it clear that organisations or individuals who hold your personal data owe you a duty of care. If you suffer damage through the mishandling of your personal information, then you may be entitled to claim compensation through the Courts and this is a matter for you and your legal advisers. The Commissioner has no function in relation to the taking of such proceedings or in the giving of legal advice.

To assist the Commissioner in exercising his / her functions, he or she is assigned certain important powers under the Data Protection Acts, 1988 and 2003, and under the Electronic Communications Regulations, S.I. 535 of 2003 (as amended by SI 526 of 2008).

a) Investigations by the Data Protection Commissioner

Under section 10 of the Data Protection Acts, 1988 and 2003, the Commissioner will investigate any complaints which he receives from individuals who feel that personal information about them is not being treated in accordance with the Act, unless he is of the opinion that such complaints are "frivolous or vexatious". The Commissioner notifies the complainant in writing of his decision regarding the complaint. The Commissioner's decision can be appealed to the Circuit Court.

The Commissioner may also launch investigations on his own initiative, where he is of the opinion that there might be a breach of the Act, or he considers it appropriate in order to ensure compliance with the Acts.

b) The Commissioner's Power to Obtain Information
Under section 12 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may require any person to provide him with whatever information the Commissioner needs to carry out his functions, such as to pursue an investigation. The Commissioner exercises this power by providing a written notice, called an "information notice", to the person.
A person who receives an information notice has the right to appeal it to the Circuit Court.

Failure to comply with an information notice without reasonable excuse is an offence. Knowingly to provide false information, or information that is misleading in a material respect, in response to an information notice is an offence. No legal prohibition may stand in the way of compliance with an information notice. The only exceptions to compliance with an information notice are (i) where the information in question is or was, in the opinion of the Minister for Justice, Equality and Law Reform, or in the opinion of the Minister for Defence, kept for the purpose of safeguarding the security of the State, and (ii) where the information is privileged from disclosure in proceedings in any court.

c) The Commissioner's Power to Enforce Compliance with the Act

Under section 10 of the Data Protection Act, 1988, the Data Protection Commissioner may require a data controller or data processor to take whatever steps the Commissioner considers appropriate to comply with the terms of the Data Protection Act, 1988. Such steps could include correcting the data, blocking the data from use for certain purposes, supplementing the data with a statement which the Commissioner approves, or erasing the data altogether. The Commissioner exercises this power by providing a written notice, called an "enforcement notice", to the data controller or data processor. A person who receives an enforcement notice has the right to appeal it to the Circuit Court.
It is an offence to fail or refuse to comply with an enforcement notice without reasonable excuse.

d) The Commissioner's Power to Prohibit Overseas Transfer of Personal Data

Under section 11 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may prohibit the transfer of personal data from the State to a place outside the State. The Commissioner exercises this power by providing a written notice, called a "prohibition notice", to the data controller or data processor.
In considering whether to exercise this power, the Commissioner must have regard to the need to facilitate international transfers of information.
A prohibition notice may be absolute, or may prohibit the transfer of personal data until the person concerned takes certain steps to protect the interests of the individuals affected. A person who receives an prohibition notice has the right to appeal it to the Circuit Court.
It is an offence to fail or refuse to comply with a prohibition specified in a prohibition notice without reasonable excuse.

e) The Powers of "Authorised Officers" to Enter and Examine Premises

Under section 24 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may appoint an "authorised officer" to enter and examine the premises of a data controller or data processor, to enable the Commissioner to carry out his functions, such as to pursue an investigation. The authorised officer, upon production of his or her written authorisation from the Commissioner, has the power to:
? enter the premises and inspect any data equipment there
? require the data controller, data processor or staff to assist in obtaining access to data, and to provide any related information
? inspect and copy any information
? require the data controller, data processor or staff to provide information about procedures on complying with the Act, sources of data, purposes for which personal data are kept, persons to whom data are disclosed, and data equipment on the premises.
It is an offence to obstruct or impede an authorised officer; to fail to comply with any of the requirements set out above; or knowingly to give false or misleading information to an authorised officer.

f) Appeals to the Court

Disclaimer: If you are contemplating taking an appeal against a decision of the Commissioner, or against the exercise of the Commissioner's powers, it is recommended that you seek independent legal advice. Note that the material contained in this section is provided for general information purposes only, and does not purport to be legal advice or a definitive interpretation of the law.
Under section 26 of the Data Protection Acts, appeals can be made to the Circuit Court against:-
? a requirement specified in an information notice
? a requirement specified in an enforcement notice
? a prohibition specified in a prohibition notice
? a refusal by the Data Protection Commissioner to accept an application for registration, or for renewal of registration, or for an amendment of registration details
? a decision of the Data Protection Commissioner in relation to a complaint by an individual.
Appeals to the court must normally be made within 21 days from the service of the notice, or from the date of receipt of the refusal or decision. The decision of the court is final, although an appeal against the court's decision may be brought to the High Court on a point of law.

g) Prosecution of offences under Data Protection Acts and under S.I. 336 of 2011 (Electronic Privacy Regulations).
Section 30 of the Data Protection Acts provides that the Commissioner may bring summary proceedings for an offence under the Acts. The Commissioner also has the power to prosecute offences in relation to unsolicited marketing under S.I. 535 of 2003 (Electronic Communications Regulations) (as amended by SI 526 of 2008).

1.7 What is the difference between FOI and Data Protection?

The Freedom of Information Acts grant every person a right, subject to certain restrictions, to access information held by Government Departments, agencies and other designated bodies in receipt of State funding. The FOI Acts also allow for persons to seek access to their own data held by such bodies.

The requirements of the Data Protection Acts apply to all legal entities in this jurisdiction whether Government, private, voluntary or charitable that control personal data. More guidance on this is available at the following link: Are you a Data Controller?

The Acts place obligations on such entities in terms of how they process personal data. One of these obligations is to give a person a copy of their personal data on request. This right to access personal data is subject to very limited exemptions.
When a public body covered by Freedom of Information legislation receives an FOI request from a person for their own information, they are required to also consider the request under data protection requirements and give the person the maximum amount of their information taking account of both sets of legislation. More detailed guidance is available here Data Protection and Freedom of Information in the Public Sector

1.8 Under what circumstances can I disclose personal data without the consent of the data subject?

Disclosure of personal data without the individual data subject's consent is permitted in certain limited circumstances laid down in the Data Protection Acts (mainly Sections 8 and 2A). These include where disclosure is necessary to prevent injury or damage to the health of an individual, where such disclosure is required by law or where disclosure is made to the Gardaí in relation to a criminal investigation. The law also permits such disclosure where the "legitimate interests" of the data controller are involved and are not outweighed by the rights of the individual in a particular case.

1.9 What is the position in relation to personal data already in the public domain?

Section 1 (4) (b) of the Data Protection Acts provides that the Acts do not apply to personal data consisting of information that the person keeping the data is required by law to make available to the public. A key point here is that the exemption from data protection requirements only relates to the information in the hands of those public bodies that are obliged to make it available. Any other entity seeking to use such information once in the public domain must comply with the standard requirements of data protection.