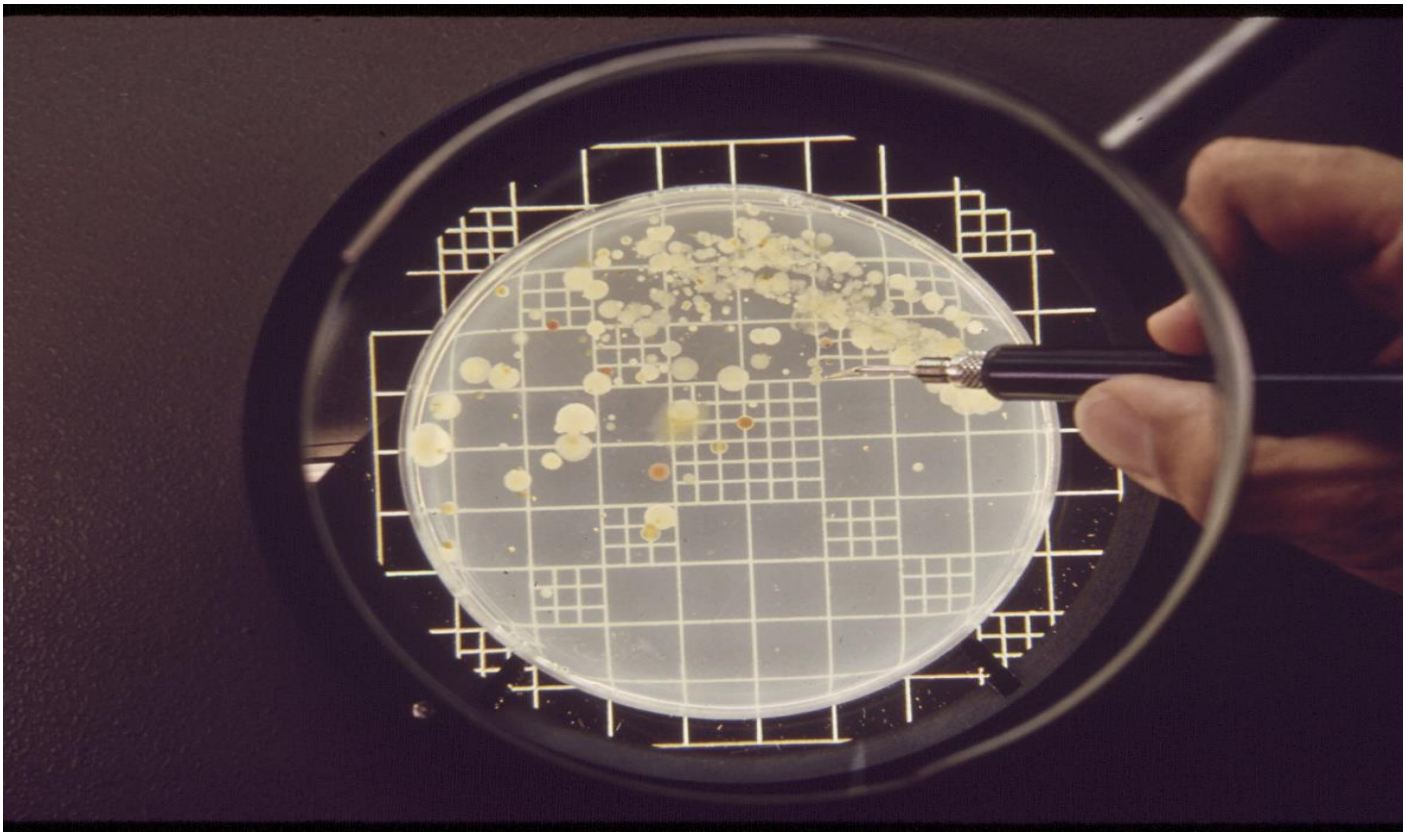
Deloitte.

Data Protection Bill 2018

Key points of the recently published Data Protection Bill

February 2018



Introduction

The highly anticipated text of the Irish Data Protection Bill 2018 has been published.

The Bill supplements and gives further effect under Irish law to the General Data Protection Regulation (2016/679) (the 'GDPR') as well as the Law Enforcement Directive (2016/680) and, for the most part, repeals the current Data Protection Act 1998 and 2003. While still subject to amendments by the Oireachtas before enactment, this update explores the boundaries of the current text of the Bill and points out key provisions under it.

Key points of the Bill are the particulars of the establishment of the *Data Protection Commission*, the setting out of certain *restrictions to data subject rights* and details on how the Regulation will be enforced, including the *powers of the Commission* to inspect and investigate and *impose administrative fines* as well as *personal liability* in some cases for contravening requirements.

We summarise at a high level these key points under the Bill as follows:

The Data Protection Acts 1998 and 2003

While the Bill repeals the current Data Protection Acts, it does not repeal it in its entirety. The provisions under the 1998 Act which relate to processing of personal data for purposes of national security, defence and international relations of the State will remain effective. The Act will also continue to apply to any complaint or investigation under Section 10 of the Acts relating to enforcement of the Acts.

The Data Protection Commission

The Office of the Data Protection Commissioner will be known as the Data Protection Commission. It will be independent in the performance of its functions, will have all powers that are necessary for the performance of these functions as the supervisory authority and shall regulate its own procedures.

The Bill allows for a three member Commission and each Commissioner shall be appointed for a period of at least 4 years but not more than 5 years and may be reappointed for a further similar period. One of the three Commissioners will be appointed as chairperson and will have casting voting rights.

The Commission will be accountable to an Oireachtas Committee.

Enforced Access Requests

Requesting an individual to make an access requests for the purposes of recruitment, continued employment or a contract for the provision of services will be an offence and a person who contravenes this will be subject to a fine or imprisonment.

Age of Consent

The age of consent for a child in relation to information society services will be 13 years of age.

Suitable and Specific Measures

Throughout the Bill, it is clear that there is frequent reference within provisions to 'suitable and specific measures for processing'.

Those measures may include:

- gaining explicit consent of the data subject for the processing of his/her personal data;
- limitations on access to personal data that is being processed within a work environment;
- strict time limits for the erasure of personal data and mechanisms to ensure such limits are observed; and
- specific and targeted training for individuals involved in processing operations.

In addition, the Bill underpins a risk based approach (that has regard to the state of the art, context, nature, scope and purposes of the personal data processed) to the application and use of logging mechanisms, pseudonymisation, encryption and other technical and organisational measures designed to ensure that the processing is carried out in accordance with the GDPR. This includes processes for testing and evaluating the effectiveness of such measures.

Further, these 'suitable and specific measures' may be identified explicitly in Regulations made by a Minister of the Government or the Data Protection Commission.

Lawful Processing under the Bill

The Bill stipulates the types of processing of personal data that will be lawful to the extent necessary in a number of instances. None of these are surprising and are listed in the table below.

One key change however is in relation to the processing of special categories of personal data for insurance and pension purposes. The processing of health data shall be lawful where the processing is necessary and proportionate in relation to an insurance policy or life assurance, health policies, an occupational pension, retirement annuity contract or any other pension arrangement or the mortgaging of property.

Lawful Processing of personal data	Lawful Processing of special categories of personal data	Lawful Processing relating to criminal convictions and offences
Processing for a task carried out in the **public interest**, or in the **exercise of official authority**, including where the personal data is processed and disclosed in relation to the preservation of the Common Travel Area and the controller is an Irish air carrier, an air carrier or a sea carrier.	Processing of special categories of personal data for purposes of **employment and social welfare law** where this is necessary for the performance of any right or obligation which is conferred or imposed by law in connection with employment and social welfare law.	Processing of personal data relating to **criminal convictions and offences** under the control of official authority or where explicit consent exists shall be lawful.
Processing for purpose other than the purpose for which data was collected shall be lawful for the prevention of a threat to **national security, defence or public security,** prevention of and investigation or prosecution of criminal offences.	Processing of special categories of personal data for the purpose of **legal advice and legal proceedings**.	
Processing, including processing of special categories of personal data, for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.** The processing under these purposes must respect the principle of data minimisation and where they can be fulfilled by processing non-identifiable data, the processing should be carried out in that manner.	Processing of personal data revealing **political opinions for the purpose of electoral activities** in relation to compiling data by a political party, a body established by or under an enactment or a candidate for election to or holder of elective political office.	
Personal data may be processed for the purposes of disclosing it under a **Freedom of Information** request.	Processing of special categories of personal data for the purposes of **administration of justice** and **performance of functions** which respects the essence of the right to data protection and is necessary and proportionate to the purposes.	
	Processing of special categories of personal data for reasons of **substantial public interest** where these are underpinned by regulations made specifically.	
	Processing of special categories of personal data where it is necessary for the purposes of **preventative or occupational medicine,** for the assessment of the **working capacity of an employee,** for **medicinal diagnosis**, for the provision of **medical care, treatment or social care**, for the **management of health**	

	or social care systems or services or under a contract with a health professional. The processing shall be lawful if undertaken by or under the responsibility of a health practitioner or an individual under a duty of confidentiality to the data subject equivalent to a health practitioner;	
	Processing of special categories of personal data for purposes of public interest in the area of **public health** including protecting against serious cross-border threats to health and ensuring high standards of quality and safety of health care and of medicinal products and medical devices	

Data Subject Rights and Restriction of Rights

The Bill underpins the rights to information and access that a data subject can make as well as the rights to restriction of processing, erasure and rectification under the GDPR. The Bill goes further to call out certain rights and restrictions explicitly, as follows:

- Right of access to results of examination: an individual can make a request in relation to the results of an examination that he or she was a candidate of on the later of (a) the date of first publication of the results or (b) the date of the request.

- Right to object to automated decision making including profiling: this right shall not apply where the automated decision is authorised or required by an enactment and where the effect of that decision is as a result of a request by the data subject or where the controller has taken all adequate steps to safeguard the legitimate interests of the data subject. The safeguarding of legitimate interests includes making arrangements so that the data subject can make representations to the data controller in respect of the decision.

- Right to object to direct marketing: this does not apply where the direct mailing is carried out in the course of electoral activities subject to certain conditions;

- Right to object to processing for electoral activities: this shall not apply to processing carried out in the course of electoral activities by a political party, a body established by or under an enactment or a candidate for election to, or holder of, elective political office.

- Restriction of rights in relation to archiving: Certain data subject rights under the GDPR will not apply where the processing of personal data is necessary for archiving purposes in the public interest.

The Bill goes on to set out in detail where restrictions to data subject rights under the GDPR may be necessary. These include where a restriction is

necessary in line with specific regulations made by a Minister of Government (a) in relation to the protection of data subjects where the application of the rights would cause serious harm, or (b) where personal data is kept for carrying out social work by a public authority, public body or voluntary organisation. In addition, regulations may be made restricting rights where it is deemed necessary for safeguarding important objectives of public interest.

The box below lists the instances where restrictions on data subject rights may be necessary.

-to safeguard cabinet confidentiality, judicial independence and court proceedings, parliamentary privilege, national security, defence and the international relations of the state;

- for the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties;

- for the administration of any tax, duty or other money due or owing to the State, a local authority or other public authority or body;

- in contemplation of or establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure;

- for the enforcement of civil law claims, including matters relating to any liability of a controller or processor in respect of damages, compensation or other liabilities or debts in relation to the claim;

- for the purposes of estimating the amount of the liability of a controller on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of those rights or obligations would be likely to prejudice the interests of the controller in relation to the claim;

- the personal data relating to the data subject consist of expressions of opinion about the data subject by another person given in confidence or on the understanding that it would be treated as confidential to a person who has a legitimate interest in receiving the information;

- the personal data concerned are kept by the Commission or the Information Commissioner for the performance of the functions of the Commission or Information Commissioner, as the case may be.

Enforcement of the Regulation

- **Complaint**

The Bill includes a provision which allows for the data subject to mandate a not-for-profit body, organisation or association to lodge a complaint with the Commission or bring a judicial action on their behalf. In respect of the judicial action brought on behalf of the data subject, the court can grant relief by way of an injunction or declaration but cannot award compensation for damage suffered by the data subject.

The powers of inspection, investigation, audit and enforcement that the Commission will have are set out in the Bill as follows:

- **Inspection and Investigation**

The Commission may appoint as many members of staff as necessary to be an authorised officer with powers to enter any organisation (with the consent of the occupier or with a search warrant) where any processing of personal data is carried out. The officer can search and inspect the organisation and any relevant documents or records as well as require any person to produce all records in relation to the processing of personal data. The authorised officer can secure these records for later inspection or retain as necessary for carrying out the inspection.

In carrying out the functions, the authorised officer may operate or gain access to any equipment as necessary for the purposes of the inspection. Any person who impedes the authorised officer from carrying out his/her duties in any way shall be guilty of an offence and liable to a fine or imprisonment.

The Commission or authorised officer may also serve an information notice to a data controller or processor mandating that controller or processor to provide the Commission any information specified in the notice within a period of 28 days. If the data controller or processor fails to comply, they will be guilty of an offence and liable to a fine or imprisonment.

In addition to the above powers, the Commission may instigate an investigation where it considers it appropriate and suspects there is an infringement.

- **Audit**

The Bill stipulates that the Commission may carry out or cause to be carried out by a third party an audit of a data controller or processor to determine compliance with all data protection requirements.

- **Enforcement**

If the Commission is of the opinion that a data controller or processor has contravened or is contravening any relevant provisions, an enforcement notice requiring the controller or processor to take one or more steps shall be issued. The Commission may decide to impose an administrative fine on a data controller or processor who fails to comply with a requirement specified in the enforcement notice or may deem the controller or processor guilty of an offence and liable for a fine or imprisonment.

- **Report**

In order to effectively monitor compliance with requirements, the Commission may require the data controller or processor to provide a report, information or documentation to the Commission on any matter specified in a written notice. The report may be prepared by a person nominated by the data controller or processor and approved by the Commission. A person who impedes the preparation of the report in any manner as set out under the Bill shall be guilty of an offence and liable to a fine or imprisonment.

Administrative Fines

The Bill clearly states that the Commission has the power to decide to impose an administrative fine where appropriate and similarly can decide not to impose a fine where the same controller or processor is the subject of a criminal penalty in relation to the same infringement.

A key provision in the Bill outlines that Public Sector Bodies will be exempt from administrative fines unless in direct competition with private companies within the meaning of the Competition Act 2002.

In relation to the fines that can be imposed within the private sector, there will be an appeals process to the Circuit and High courts depending on the amount of the fine.

Offences

The Bill sets out a number of instances that will be deemed a criminal offence and liable to a fine or imprisonment. These include:

- Unauthorised disclosure of personal data by a data processor;
- Disclosure of personal data obtained without authority of the data controller or processor; and
- Offences by directors, managers, secretaries or other officers of bodies corporate which are proved to be committed with consent or connivance of or attributable to neglect of such persons.

Publication

The Commission shall publish details on any conviction of a person for contravening the Data Protection Act, any particulars in relation to the imposition of administrative fines or suspension of the transfer of personal data to a third country or international organisation or by order of the Court. In addition, if the Commission deems it in the public interest, they may publish particulars of any report from an investigation or audit.

Law Enforcement Directive

Part 5 of the Bill sets out the requirements and exceptions in relation to the processing of personal data for law enforcement purposes. Some key points to note from this are as follows:

Records of Processing: The records of processing requirements under the Bill go one step further than the requirements under GDPR and include keeping a record of whether or not processing involves the use of profiling.

Data Logging: The Bill introduces a requirement to keep a data log in instances where a data controller or processor carries out processing of personal data by automated means. A data log of these automated processing operations within automated processing systems must be created and maintained. The criteria that is required to be captured within that data

log is set out clearly in the Bill under Article 76. This log may be requested to be made available to the Commission for inspection and examination.

A key part of this section however, states that this data logging requirement shall not apply in respect of an automated processing system established on or before 6 May 2016 -

1. Prior to 6 May 2023 where compliance would involve a disproportionate amount of effort; or
2. Prior to 6 May 2026 where compliance would cause serious difficulties for the operation of the automated processing system to which the data log relates. A controller or processor intending to rely on this must notify the Minister (for Justice and Equality) on or before 31 December 2022 and the notification must include a description of the serious difficulties intended to be relied upon.

For more information on the draft Data Protection Bill and it's progress to finalisation and enactment or to hear more about our GDPR services, please contact the Deloitte Ireland Data Privacy Services team.

Contact

Sean Smith
Partner| Risk Advisory
Email: seansmith1@deloitte.ie

Donal Murray
Director | Risk Advisory
Email: donmurray@deloitte.ie

Nicola Flannery
Senior Manager | Risk Advisory
Email: niflannery@deloitte.ie

Deloitte.