

## **Data Protection Act 2018**

### **Explanatory Memorandum**

#### **Background**

Following protracted negotiations, the General Data Protection Regulation (“GDPR”) was agreed in early 2016 and entered into force across the European Union on 25 May 2018 (Regulation (EU) 2016/679). An accompanying law enforcement Directive (“Directive”), which establishes data protection standards for the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection and prosecution of criminal offences and the execution of criminal penalties was also agreed in early 2016 (Directive (EU) 2016/680). The Directive required transposition into national law by May 2018.

Both the GDPR and Directive have a legal basis in Article 16 of the Treaty on the Functioning of the European Union, and they provide for significant reforms to earlier data protection rules which were based on the EU’s 1995 Data Protection Directive. Both instruments generally provide for higher standards of data protection for individuals (“data subjects”) and impose more detailed obligations on bodies in the public and private sectors that process personal data (“controllers” and “processors”). They also increase the range of possible sanctions for infringements of these standards and obligations.

The GDPR seeks to provide for a more uniform interpretation and application of data protection standards across the EU, thereby providing a level playing field for those doing business in the EU digital market. The European Data Protection Board (“the Board”), comprising representatives of the data protection authorities of all Member States, will play an important role in this respect (see Articles 70 and 51 of the GDPR and Directive respectively).

While many key data protection concepts and principles remain broadly similar to those set out in the Data Protection Acts 1988 and 2003 (which have given effect in national law to the 1981 Council of Europe Data Protection Convention (Convention 108) and the EU’s 1995 Data Protection Directive respectively), both the GDPR and Directive introduce new elements and some enhancements that require detailed consideration by all those involved in the processing of personal data. At the heart of both is a “risk-based” approach to data protection. This means that each individual controller and processor is required to put appropriate technical and organisational measures in place in order to ensure – and, importantly, to be able to demonstrate – that their processing of personal data complies with the updated data protection standards. For the purposes of assessing the nature, level and likelihood of risks for the rights and freedoms of data subjects, they must take account of the nature, scope, context and purposes of the data processing. In certain cases, this will require

the carrying out of data protection impact assessments, and where mitigation of risk is not possible prior consultation with the Data Protection Commission will be mandatory.

Both the GDPR and Directive place greatly increased emphasis on the transparency of processing, the responsibility of the controller and processor for compliance with data protection standards, and the need for appropriate security standards to be implemented in order to protect against data breaches such as unauthorised or unlawful processing and accidental loss, destruction or damage.

Both instruments impose an obligation on all public authorities and bodies, as well as certain private sector bodies, to designate a Data Protection Officer with responsibility to oversee data processing operations, and to report data breaches to the relevant data protection authority. The GDPR also limits the grounds for lawful processing of personal data by public authorities and bodies. For example, depending on the circumstances, an individual's consent to the processing of his or her personal data may not provide a reliable basis for such processing by a public authority. Moreover, the so-called "legitimate interests" ground will no longer be available to public authorities when acting in that capacity (Article 6.1(f)).

Both the GDPR and Directive provide for increased supervision and enforcement of data protection standards by the data protection authority. The GDPR provides for the possible imposition of substantial administrative fines (up to €10 million or €20 million, or 2% or 4% of total worldwide annual turnover in the preceding financial year). In the case of a public authority or body that is not an undertaking within the meaning of the Competition Act 2002, the amount of an administrative fine shall not exceed €1 million. Both the GDPR and Directive provide that any data subject who has suffered material or non-material damage because of a breach of his or her data protection rights shall have the right to seek compensation in the courts.

### **Purpose and structure of the Act**

The key purposes of the Act are as follows:

- to give further effect to the GDPR in areas in which Member State flexibility is permitted;
- to transpose the Directive into national law;
- to establish the Data Protection Commission as the State's data protection authority with the means to supervise and enforce the data protection standards enshrined in the GDPR and Directive in an efficient and effective manner, and
- to enact consequential amendments to various Acts that contain references to the Data Protection Acts 1988 and 2003.

The Act comprises the following Parts:

- Part 1 (sections 1 to 8) contains a number of standard provisions, e.g. citation, commencement and definitions. Section 7 makes provision for repeals, while section 8 defines the residual scope of the Data Protection Act 1988.

- Part 2 (sections 9 to 27) establishes the Data Protection Commission to replace the Data Protection Commissioner as the State’s data protection authority. Its primary task is to act as the supervisory authority for the GDPR and the Directive. Establishment of the Commission, comprising at least one commissioner and not more than 3, is a future-proofing provision to allow, should the need arise in future, for the appointment of additional commissioners in response to an increased Commission workload.
- Part 3 (sections 28 to 61) gives further effect to the GDPR in a number of areas, mainly affecting the public sector, in which the Member States retain a margin of flexibility. In certain cases, this involves the creation of a regulation-making power that will permit the making of more detailed regulations in due course.
- Part 4 (sections 62 to 68) contains a number of provisions that are consequential on replacement of the Data Protection Commissioner with the Data Protection Commission.
- Part 5 (sections 69 to 104) transposes the Directive’s provisions in national law.
- Part 6 (sections 105 to 156) contains provisions dealing with enforcement of the obligations and rights set out in the GDPR and Directive by the Data Protection Commission. The intention is to ensure effective supervision and enforcement mechanisms, together with procedural and due process safeguards.
- Part 7 (sections 157 to 164) contains a number of miscellaneous provisions, mainly concerning the application of data protection rules to the courts and a number of related legal matters.
- Part 8 (sections 165 to 232) contains consequential amendments to a significant number of Acts.

### **Part 1 – Preliminary and general**

Sections 1, 2, 5 and 6 contain standard provisions. Section 3 re-enacts, with amendments, section 1(3) of the Data Protection Act 1988, which permits an appropriate authority (within the meaning of the Civil Service Regulation Act 1956), to appoint a civil servant as a controller, and permits the Minister for Defence to designate an officer of the Permanent Defence Force as a controller.

Section 4 re-enacts section 4(13) of the Data Protection Act 1988; it prohibits a practice known as “enforced data subject access”, whereby an individual may be required, in the employment context, to present personal data obtained by him or her on foot of an access request to his or her employer to a possible future employer.

Sections 7 and 8 are concerned with the Data Protection Acts 1988 and 2003. Section 7 provides for repeals of certain provisions in both Acts and for the revocation of specified Statutory Instruments, while section 8 provides for the residual scope of the 1988 Act. Subsection (4) of section 7 and subsection (2) of section 8 provide that the 1988 Act will continue to apply to complaints made, investigations commenced and contraventions of the 1988 Act before the commencement of the 2018 Act. Subsection (3) of section 8 provides that any investigation commenced by the Data Protection Commissioner under section 10 of the 1988 Act before commencement of the 2018 Act shall be completed by the Data Protection Commission.

While Article 2.2(a) of the GDPR provides that its provisions do not apply to the processing of personal data in the course of an activity falling outside the scope of EU law, there has been some uncertainty about the extent of that exclusion in light of evolving Court of Justice case law concerning the scope of EU law. A detailed analysis of relevant case law indicates that the exclusion in Article 2.2(a) appears to be limited in practice to data processing in the context of national security, defence and the international relations of the State.

While national security and defence lie outside the scope of EU law, the Council of Europe's 1981 Data Protection Convention (Convention 108) is relevant to data processing for the purposes of safeguarding national security, defence and international relations in States that have ratified the Convention. The process of updating and modernising this Convention was ongoing for a number of years and was not completed until after the enactment of this Act. It is for that reason that section 8 retains relevant provisions of the 1988 Act for the purposes of data processing in the context of national security, defence and the international relations of the State.

Article 60 and recital 94 of the Directive provide that Union legal acts that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems shall remain unaffected by the Directive. This means that the Directive does not apply to Prüm measures i.e. Council Decisions 2008/615/JHA and 2008/616/JHA. Article 62 of the Directive imposes an obligation on the European Commission to review those legal acts by 6 May 2019 in order to assess the need to align them with the Directive and to make, where appropriate, the necessary proposals to amend those acts. Council Decisions 2008/615/JHA and 2008/616/JHA are given effect in the Criminal Justice (Forensic Evidence and DNA Database System) Act 2014 and the Vehicle Registration Data (Automated Searching and Exchange) Act 2018. Any amendments to those Acts in the Data Protection Act 2018 would pre-empt the findings of the Commission and could result in further amendments being required following the publication of the Commission report. Section 8 of the Act therefore provides that the 1988 Act will continue to apply in the case of these Acts.

## **Part 2 – Data Protection Commission**

The GDPR and this Act will have far-reaching implications for the workload of the State’s data protection authority. The volume of its supervisory, investigative and enforcement work will increase and the number of data subject complaints are likely to increase and become more complex, especially those with cross-border aspects. Both the GDPR and Directive confer a range of additional tasks and powers, including investigative, corrective, authorisation and advisory powers, on supervisory authorities.

The GDPR contains a “consistency mechanism” – sometimes referred to as a “One-Stop-Shop” – which is intended to streamline the handling of cross-border data protection complaints. The mechanism is based on the concept of a “lead” supervisory authority, meaning the data protection authority of the Member State in which a controller’s “main” or only EU establishment is located. It means that complaints will generally fall to be investigated by the data protection authority of that Member State, irrespective of the origin of the complaint. That authority may request assistance from other data protection authorities for investigation purposes, but the initial conclusion as to whether or not an infringement of data protection law has occurred, or is occurring, will be that of the lead supervisory authority.

Before arriving at any final decision in cross-border cases, the lead supervisory authority must submit a draft decision to the data protection authorities of other Member States with an interest in the case, e.g. either because the complaint has originated in that Member State or the controller concerned has other establishments there. The lead supervisory authority must have regard to any relevant and reasoned objections to the draft decision submitted by other concerned supervisory authorities, and if consensus cannot be reached, the case will come before the European Data Protection Board for a binding decision.

This is the backdrop to Part 2 of the Act which provides for the establishment of the Data Protection Commission, with at least one but not more than 3 Commissioners. The number of cross-border cases coming before the Commission is likely to increase with the entry into force of the GDPR because of the presence of a significant number of multinational companies providing their digital services to data subjects across the EU from an establishment in the State.

Significant increases in levels of financial and staffing resources have been allocated to the Data Protection Commissioner in recent years in order to prepare for the expected workload increases. Staff resources have almost trebled from 30 in 2013 to 85 at the end of 2017. Additional funding of €4 million in 2018 will bring the overall budget to about €11.7 million, and this will facilitate the recruitment of additional staff and bring total numbers to about 140. There are no plans at present to increase the number of Commissioners.

Sections 9, 10 and 11 are standard provisions. Section 12 outlines the functions of the Commission, while section 13 provides for the delegation of certain Commission functions.

Section 14 transfers functions from the Data Protection Commissioner to the Commission, while section 15 deals with matters relating to its membership, including the appointment of commissioners. Sections 16, 17 and 18 contain ancillary provisions. Section 19 provides for accountability to Oireachtas Committees, while section 25 provides that the Commissioner, or where more than one Commissioner has been appointed, the chairperson, is the Accounting Officer under the Comptroller and Auditor General Acts. Sections 20 to 22 deal with staffing and with superannuation matters. Sections 23 and 24 provide for production of annual accounts and annual report respectively, while sections 26 and 27 contain provisions concerning the prohibition on disclosure of confidential information in the possession of the Commission while performing functions under the GDPR and this Act.

### **Part 3 - Data Protection Regulation**

This Part of the Act, comprising three chapters, gives further effect to a number of Articles in the GDPR where Member States retain a margin of flexibility.

#### Chapter 1

This Chapter contains a number of general measures. While the GDPR does not generally permit the imposition of fees by data protection authorities, Article 57 allows them to charge a reasonable fee, based on administrative costs, where data subject requests are manifestly unfounded or excessive, in particular because of their repetitive character. As an alternative, the authority concerned may refuse to act on such requests. Section 28 contains a provision that allows the Commission to prescribe fees for such cases. It also allows for possible fees for the performance of certain potentially resource-intensive functions, such as the authorisation of contractual clauses for transfers of personal data to third countries and international organisations under Article 57.1(r), or the approval of binding corporate rules to permit inter-company transfers of personal data under Article 57.1(s).

Section 29 provides that references to “child” in the GDPR shall be taken to refer to a person under the age of 18 years. This is in line with the definition in Article 1 of the UN Convention on the Rights of the Child.

Apart from Article 8 (see below), the GDPR incorporates a number of enhanced protections for the personal data of children. These include:

- Article 6.1(f), which generally permits processing of personal data where necessary for the purposes of the “legitimate interests” of a controller that is not a public authority, may not be relied upon where such interests are overridden by the interests or fundamental rights and freedoms of a data subject, in particular where the data subject is a child;
- Article 12 imposes high standards of transparency on controllers when providing information to data subjects, in particular for any information addressed to a child;
- Article 17 (Right to erasure) underlines the particular relevance of the right to erasure where processing is based on consent given when the data subject was a child and not, therefore, fully aware of the risks involved;

- Article 40 makes general provision for codes of conduct; specific mention is made to a possible code concerning the provision of information to, and the protection of, children, and the manner in which the consent of holders of parental responsibility over children is to be obtained for the purposes of Article 8;
- Article 57, which requires data protection authorities to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to data processing, states that activities addressed specifically to children must receive specific attention.

Section 30 makes it an offence to process personal data of a child for the purposes of direct marketing, profiling or micro-targeting. It has not been possible to commence this section as it goes beyond the margin of discretion afforded to Member States in giving further effect to the GDPR and would give rise to a substantial risk of infringement proceedings against the State pursuant to Article 258 of the Treaty on the Functioning of the European Union, and exposure of the State to sanctions.

For the purposes of Article 8 of the GDPR, section 31(1) specifies 16 years of age as the “digital age of consent”. It means that where information society services – defined in Article 4(25) – are offered directly to children, the processing of a child’s personal data will be lawful only if, and to the extent that, consent is given or authorised by the holder of parental responsibility over the child. In such cases, the service provider must make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility. Subsection (3) provides for a review of the operation of this provision no later than 3 years after its coming into operation.

Section 32 makes provision for the drawing up and implementation of codes of conduct intended to contribute to the proper application of the GDPR with regard to the protection of children, as permitted under Article 40 of the GDPR. Subsection (2) provides for consultations with relevant stakeholders, including children and bodies representing their interests, during that process.

Section 33 makes specific provision for an enhanced “right to be forgotten” in the case of children in accordance with Article 17 of the GDPR.

Section 35 designates the Irish National Accreditation Board as the accreditation body in the State for the purposes of Article 43 of the GDPR; this allows accreditation bodies to issue and renew certifications for the purposes of certification mechanisms, such as data protection seals and marks. The intention is that such mechanisms could be used by controllers and processors for the purposes of demonstrating compliance with the GDPR by controllers and processors.

Sections 34 and 37 establish regulation-making powers for the purposes of Articles 37.4 and 49.5 of the GDPR respectively. Article 37.4 allows EU or Member State law to extend the range of controllers and processors that are required to designate a data protection officer, while Article 49.5 allows Member States, for important public policy reasons, to set limits on

the transfer of specific categories of personal data to a third country or international organisation. Public policy reasons in this context could, for example, relate to possible detriment to individuals arising from transfer of their personal data to a third country or international organisation.

Article 6 of the GDPR provides, *inter alia*, that processing of personal data is lawful where necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Section 38(1) confirms that processing is lawful to the extent that it is necessary and proportionate for the performance of a function conferred on a controller by or under an enactment or by the Constitution, and for the administration of any non-statutory scheme, programme or funds where the legal basis is a function of a controller conferred by or under an enactment or the Constitution.

Subsections (2), (3) and (8) deal with the processing of personal data by air and sea carriers for the purposes of the Common Travel Area, while subsections (4) to (7) create a regulation-making power for the purposes of specifying data processing that is necessary for the performance of a task carried out in the public interest by a controller or which is necessary in the exercise of official authority vested in a controller. Such specification may provide, in particular, legal certainty where processing is carried out by bodies other than public authorities and bodies. Recital 45 of the GDPR refers to the possibility of processing in the public interest, or in the exercise of official authority, being carried out by controllers other than authorities or bodies governed by public law.

Section 39 provides that a specified person (i.e. a political party; a member of, or a candidate for election to, either House of the Oireachtas, the European Parliament or a local authority; or a candidate for election to the office of President of Ireland) may, in the course of electoral activities in the State, use the personal data of a data subject for the purpose of communicating in writing with the data subject. Such communication may include communication by way of newsletter or circular.

Subsections (1) and (2) of section 40 provide a legal basis for the making of representations by elected representatives where the elected representative receives a request or representation from an individual or on behalf of an individual where the individual has given consent or is unable to make the request or representation because of his or her physical or mental capacity or age. Where special categories of personal data are involved, subsection (3) will require that measures to limit access to the data be taken in order to prevent unauthorised consultation, alteration, disclosure or erasure of the data. Subsection (4) provides a legal basis for responding to representations received from elected representatives on behalf of data subjects.

Section 41 provides for the processing of personal data for certain purposes other than the purpose for which the data were collected; these include processing that is necessary and proportionate for the purposes of preventing a threat to national security and defence, or



public security; preventing, detecting, investigating or prosecuting criminal offences; and the purposes of legal claims and legal proceedings.

Statutory provisions that permit, or require, further notification or disclosure of personal data are to be found in various Acts. Under section 42 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, designated persons such as financial institutions, auditors and property service providers who know, suspect or have reasonable grounds to suspect, on the basis of information available to them, that another person has been or is engaged in an offence of money laundering or terrorist financing must report that knowledge or suspicion or those reasonable grounds to the Gardaí and the Revenue Commissioners. Under sections 2 and 3 of the Criminal Justice (Withholding of Information on Offences against Children and Vulnerable Persons) Act 2012, it is an offence to withhold any information on offences referred to in that Act. The Children First Act 2015 requires mandated persons, including health practitioners, teachers and youth workers, who know, believe or suspect that a child has been harmed, is being harmed or is at risk of being harmed, to report that knowledge, belief or suspicion to the Child and Family Agency.

Section 42 makes provision for the processing of personal data for the purposes of archiving in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 of the GDPR. Such processing should respect, in particular, the data minimisation principle in Article 5.1(c) of the GDPR. Where identification of individuals is not required for these purposes, the processing should be carried out in a manner that does not permit such identification.

Section 43 gives effect to Article 85 of the GDPR, which provides that it is for national law to reconcile the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes and for the purposes of academic, artistic and literary expression. Both the right to protection of personal data and the right to freedom of expression and information are enshrined in Articles 8 and 11 of the EU Charter of Fundamental Rights respectively. In this context, subsection (3) provides that the Data Protection Commission may refer, on its own initiative, any question of law involving consideration of whether processing of personal data is exempt from certain provisions of the GDPR on freedom of expression and information grounds to the High Court for its determination.

Section 44 gives effect to Article 86 of the GDPR, which provides that it is also a matter for national law to reconcile the right to public access to official documents with the right to data protection. The Freedom of Information Act 2014 and, in so far as personal data contained in environmental information is concerned, the European Communities (Access to Information on the Environment) Regulations 2017, contain relevant provisions.

## Chapter 2

This Chapter contains provisions that deal with the processing of special categories of personal data (i.e. “sensitive personal data” under the Data Protection Act 1988). The GDPR

(Article 9.2) permits the processing of such data in certain cases, and in other cases requires that such processing be subject to the implementation of “suitable and specific measures” to safeguard the fundamental rights and freedoms of data subjects. Section 36(1) (in Chapter 1) contains a “toolbox” of measures for possible application in such cases. Subsections (2), (3) and (4) of that section contain provisions whereby certain “toolbox” measures may be imposed by means of regulations in respect of categories of personal data, categories of controllers, or types of processing.

In this Chapter, sections 46, 52, 53 and 54 give effect to Article 9.2(b), (h), (i) and (j) and 9.4 of the GDPR respectively; they permit processing of personal data for a range of employment and health-related purposes and for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Subject to implementation of suitable and specific measures set out in section 36, section 50 provides for the processing of data concerning health for insurance and pension purposes, but only where such processing is necessary and proportionate for such a purpose.

Processing of special categories of personal data is permitted for purposes of legal advice and legal proceedings under section 47; for the purpose of certain electoral activities carried out in the State by political parties or candidates for political office in the State, or by the Referendum Commission, under section 48; and for the purpose of administration of justice and the performance of functions conferred by or under an enactment or by the Constitution under section 49.

Section 51 creates a regulation-making power whereby regulations may be made in future to permit the processing of special categories of personal data and Article 10 data (i.e. personal data relating to criminal convictions and offences, including the alleged commission of an offence and any proceedings in relation to such an offence) for reasons of substantial public interest (referred to in Article 9.2(g)). This corresponds to the regulation-making power in section 2B(b)(xi) of the Data Protection Act 1988 under which a number of regulations to permit processing of sensitive personal data have been made. In accordance with section 6(5), a draft of any such regulations must be laid before both Houses of the Oireachtas and a resolution approving them passed by both Houses before they can be made.

Section 55 gives effect to Article 10 of the GDPR, which permits the processing of personal data relating to criminal convictions and offences, whether under the control of official authority or for specified purposes under national law. Paragraphs (i) to (v) of subsection 1(b) permit processing of such data for specified purposes, while subsection (2) gives examples of processing under official authority. Subsections (3) to (5) provide for the making of regulations to permit processing for the purposes of assessing the risk of fraud and preventing fraud, for assessing the risk of bribery or corruption and preventing bribery and corruption and for ensuring network and information systems security. Section 55 is without prejudice to the provisions of the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016.

### Chapter 3

This Chapter makes provision for restrictions on the exercise of data subject rights and controller obligations in certain circumstances, as permitted, in particular, by Article 23 of the GDPR. It includes the following:

- Section 56 restricts the right of access to examination scripts and results to the date of first publication of the results; it updates a similar provision in the 1988 Act to address the implications of the Court of Justice ruling in December 2017 in the Nowak case that examination scripts are personal data for the purposes of data protection law;
- Section 57 deals with automated decision-making, including profiling, as referred to in Article 22 of the GDPR. It provides that the right of a data subject not to be subject to a decision based solely on automated processing, including profiling, which produces legal effect concerning him or her, shall not apply where the decision is authorised or required by or under an enactment and the effect of the decision is to grant a request of the data subject or in all other cases, adequate steps have been taken to safeguard his or her legitimate interests, which must include the right to make representations in relation to the decision, to request human intervention in the decision-making process and to appeal the decision;
- In recognition of the overriding importance of electoral activities for the democratic system of Government, sections 58 and 59 restrict the rights of data subjects to object to direct mailing carried out in the course of electoral activities in the State, and the right to object to processing carried out in the course of electoral activities in the State, by political parties or candidates for electoral office, or by the Referendum Commission, respectively. These restrictions are carried over from section 1 (definition of “direct marketing”) and section 6A(3)(c) of the 1988 Act. Existing restrictions on electoral activities carried out by electronic means without consent of individuals under ePrivacy regulations are not affected;
- In accordance with Article 23 of the GDPR, section 60 restricts, as far as necessary and proportionate, the obligations on controllers and rights of data subjects in certain cases for the purpose of safeguarding important objectives of general public interest. It replaces the restrictions currently set out in section 5 of the 1988 Act. Subsection (3) restricts data subject rights and corresponding controller obligations as far as necessary and proportionate to safeguard the important objectives of general public interest outlined in paragraphs (a) to (c). Subsection (3)(a)(vi) carries over section 5(1)(f) of the 1988 Act, while subsection (3)(b) carries over section 4(4A) of the same Act. The latter is important in the context of protected disclosures and other whistleblowing activity;
- Section 60(6) creates a regulation-making power whereby restrictions on data subject rights and corresponding controller obligations may also apply in the case of processing for other important objectives of general public interest, including those outlined in subsection (7). Where appropriate and relevant, such regulations must include specific provisions required by Article 23.2 of the GDPR. In accordance with section 6(5), a draft

of such regulations must be laid before both Houses of the Oireachtas and a resolution approving them passed by both Houses before they can be made.

- In accordance with Article 89 of the GDPR, section 61 provides for restrictions on the exercise of data subject rights where processing is for purposes of archiving in the public interest, scientific or historical research and statistical purposes.

#### **Part 4 – Provisions consequent to establishment of Data Protection Commission and repeal of certain provisions of the Data Protection Act 1988**

Sections 62 to 68 contain provisions that are consequent on the establishment of the Data Protection Commission, e.g. transfer of property, rights and liabilities. Arrangements for the final accounts and report of the Data Protection Commissioner are in section 66. Section 8(3) provides that any investigation commenced by the Data Protection Commissioner under section 10 of the Data Protection Act 1988 before commencement of this Act shall be completed by the Data Protection Commission and section 172 contains a number of technical amendments to the 1988 Act that are required in order to ensure continuity for any investigations commenced under that Act.

Section 68 contains technical provisions for the preservation of a number of statutory instruments made under the Data Protection Act 1988, which remain relevant and necessary. Schedule 1 contains a list of statutory instruments to be revoked.

#### **Part 5 – Processing of personal data for law enforcement purposes**

This Part of the Act, containing six chapters, transposes the Directive into national law.

##### Chapter 1

This Chapter contains the definitions applicable to this Part (section 69) and defines its scope (section 70). While many of the definitions in section 69 mirror those set out in Article 4 of the GDPR, the definition of “competent authority” makes it clear that this Part applies to a public authority that is competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the State. This includes competent authorities within the criminal justice system, such as the Gardaí, DPP, probation and welfare service, prison service, etc. It also includes other statutory bodies with powers to detect, investigate and prosecute criminal offences, such as the Health and Safety Authority, and local authorities when acting, for example, as fire authorities and prosecuting offences under the Fire Services Act 1981.

The definition of “competent authority” also includes other bodies or entities authorised by law to exercise public authority and public powers for purposes falling within the scope of this Part (paragraph (b) of definition). This is relevant to Member States in which such public

powers have been vested in non-public bodies or entities, e.g. operators of private prisons; private security services; prosecution powers vested in charities.

While this Part of the Act applies to competent authorities for these specified purposes, the GDPR applies to personal data processed by such bodies for purposes falling outside the scope of this Part, e.g. their payroll and HR activities. References to “controller” in this Part are to be understood as references to the competent authorities when processing personal data for purposes falling within the scope of this Part of the Act.

Section 70 clarifies the scope of application of this Part, making it clear that it does not apply to processing that occurs in the course of an activity falling outside the scope of EU law, processing by an EU institution, body, office or agency or processing to which section 8(1)(b) applies i.e. processing of personal data under the Criminal Justice (Forensic Evidence and DNA Database System) Act 2014 or the Vehicle Registration Data (Automated Searching and Exchange) Act 2018 to the extent that the 1988 Act is applied in those Acts.

## Chapter 2

Section 71(1) outlines the relevant data protection principles, which are broadly similar to those in Article 5.1 of the GDPR. Subsection (2) provides that processing is lawful under this Part when it is necessary for the performance of a statutory function of a controller falling within the scope of this Part and, to a lesser and limited extent, where a data subject has given consent to such processing.

The limiting conditions under which processing may be based on data subject consent are set out in subsections (3) and (4). In particular, the data subject must be informed of the intended purpose of the processing and the identity of the controller. Consent must be explicit and freely given by the data subject, and may be withdrawn by him or her at any time.

Subsection (5) provides that where a competent authority collects personal data for a purpose falling within the scope of this Part, that competent authority or another competent authority may process those data for a purpose falling within the scope of this Part other than the purpose for which the data were collected in so far as the competent body concerned is authorised to process such data for such a purpose under EU or national law, and the processing is necessary and proportionate to that purpose. Under subsection (6) processing may include archiving of the data in the public interest, scientific or historical research or statistical use if carried out for purposes falling within the scope of this Part.

Subsections (7), (8) and (9) of section 71 provide for additional safeguards concerning the erasure of personal data, and conditions applicable to processing. In line with Article 5.2 of the GDPR, and as required by Article 4.2 of the Directive, subsection (10) requires that a competent authority be in a position to demonstrate compliance with this section.

Section 72 (Security measures for personal data) specifies the need for adequate and appropriate security measures for the purposes of section 71(1)(f), while section 74 (Data quality) specifies obligations in respect of data quality. Section 73 (Processing of special

categories of personal data) contains provisions that permit the processing of special categories of personal data for purposes falling within the scope of this Part. Many of these are carried over from section 2B (Processing of sensitive personal data) of the Data Protection Act 1988, including the possibility of making regulations to permit processing of special categories of personal data for reasons of substantial public interest (subsections (2) to (6)). In accordance with section 6(5), a draft of such regulations must be laid before both Houses of the Oireachtas and a resolution approving them passed by both Houses before they can be made.

### Chapter 3

This Chapter outlines the obligations of competent authorities, i.e. controllers and processors, when processing personal data for purposes falling within the scope of this Part. Many of them, e.g. section 76 (Data protection by design and default), section 79 (Joint controllers), section 80 (Processors), section 81 (Record of data processing activities), are broadly similar to corresponding Articles in Chapter 4 of the GDPR. On the other hand, section 77 (Security of automated processing) contains a more detailed list of security measures required for automated processing systems, while section 82 (Data logging for automated processing system) imposes detailed data logging obligations in respect of automated processing systems.

Section 84 (Data protection impact assessment and prior consultation with Commission) imposes an obligation to carry out a data protection impact assessment where processing, especially processing involving new technologies, is likely to result in a high risk for the rights and freedoms of individuals. Where, despite the implementation of mitigation measures, high risk remains, there is a requirement that the Data Protection Commission be consulted. In such cases, the Commission is required to issue written advice in relation to the proposed processing. It may also, where appropriate, exercise its corrective powers.

Section 86 (Notification of personal data breach to Commission) contains detailed provisions requiring notification of all data breaches to the Commission unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Where a breach is likely to result in high risk to the rights and freedoms of individuals, section 87 (Communication of data breach to data subject) requires that they be informed in a clear manner of the breach. Where individuals have not been informed already of a data breach, the Commission may, on receiving the breach report, require that they be so notified by the controller.

Under section 88 (Data protection officer), all competent authorities (other than a court, or other independent judicial authority, acting in its judicial capacity) are required to appoint a data protection officer to carry out the functions set out in subsection (5). The data protection officer must be independent in the performance of his or her functions, be provided with all necessary resources to carry out these functions and have access to all the controller's processing operations.

## Chapter 4

This Chapter specifies data subject rights under this Part. These include the right under section 89 (Rights in relation to automated decision making) not to be subject to decisions based on automated processing, including profiling, unless the taking of the decision is authorised by law and the data subject has the possibility to make representations to the competent authority in relation to the decision and the controller has taken adequate steps to safeguard the legitimate interests of the data subject.

Section 90 (Right to information), section 91 (Right of access) and section 92 (Right to rectification or erasure and restriction of processing) contain more detailed provisions than the corresponding sections in the 1988 Act (i.e. sections 3, 4, 5, 6, 6A and 6B). Fees may no longer be imposed in respect of requests under sections 91 and 92. The provisions of section 93 (Communication with data subject) require that information be provided or made available to data subjects by a controller in a concise, intelligible and accessible form, using clear and plain language.

Section 94 (Restrictions on exercise of data subject rights) provides for restrictions on the exercise of data subject rights under sections 90, 91 and 92 where a controller is satisfied that restricting the exercise of the right constitutes a necessary and proportionate measure in a democratic society, with due regard for the fundamental rights and legitimate interests of data subjects, in order to safeguard important objectives of public interest. These include avoiding obstruction to official or legal inquiries, investigations or procedures, or avoiding prejudice to the prevention, detection, investigation or prosecution of criminal offences. Subsections (2) and (3) outline relevant public interest objectives.

Where the exercise of a data subject right is restricted under section 94, a data subject may request the Data Protection Commission, as permitted under section 95 (Indirect exercise of rights and verification by Commission), to carry out a verification or review and inform the data subject concerned.

## Chapter 5

This Chapter contains a number of provisions that are intended to facilitate the transfer of personal data to competent authorities in third countries and international organisations for purposes that fall within the scope of this Part. Transfers in such cases are subject to appropriate safeguards and these may be provided by means of European Commission adequacy decisions (section 97) or appropriate safeguards (section 98). Section 99 outlines a range of derogations applicable to specific situations, e.g. a transfer of personal data is necessary in order to protect vital interests of a data subject or another individual, or otherwise to safeguard the legitimate interests of a data subject. In these cases, details of the transfer, including the reasons for it, must be kept and made available to the Data Protection Commission on request. Section 100 provides, exceptionally, that a direct transfer of personal data may be made in an individual case to a recipient in a third country that is not a competent authority under certain conditions; these include where the transfer is necessary for a purpose falling within the scope of this Part, the transfer is in the public interest, and

transfer to a competent authority in the third country concerned would be ineffective or inappropriate. In such cases, the relevant competent authority of the third country concerned should normally be informed of the transfer, as well as the Data Protection Commission.

## Chapter 6

Sections 101 to 104 contain provisions concerning the role of the Data Protection Commission under Part 5. Section 101(1) specifies the functions of the Commission under this Part, having regard to Article 46 of the Directive. These functions are broadly similar to those set out in Article 57.1 of the GDPR. The Commission's powers to advise and issue opinions under this Part are set out in section 102 (other powers are set out in Part 6). The sections in this Part and Part 6 take account of the requirements in Article 47 of the Directive that the supervisory authority be vested with effective investigative, corrective and advisory powers. Unlike the GDPR, the Directive does not provide for the imposition of administrative fines in the case of infringements. Sections 103 and 104 deal with mutual assistance matters.

## **Part 6** **Enforcement of Regulation and Directive**

This Part, containing eight chapters, deals with supervision and enforcement of the GDPR and the Directive. Both the GDPR (Article 58.4) and the Directive (Article 47.4) provide that the exercise of powers conferred on the supervisory authorities shall be subject to appropriate safeguards, including effective judicial remedy and due process.

### Chapter 1

Section 105 (Interpretation) contains a number of relevant definitions, while section 106 provides for the service of documents by the Data Protection Commission for the purposes of its supervision and enforcement activities.

### Chapter 2

This deals with enforcement of the GDPR. Section 107 contains a number of relevant definitions, including "complaint", "complainant" and "corrective power". Section 108 contains general provisions for the handling of complaints lodged by or on behalf of a data subject, while section 109 outlines in more detail the manner in which complaints will be handled. Following examination of a complaint, the Commission will take such action as it considers appropriate in the circumstances of the case. Where the Commission considers that there is a reasonable prospect of the parties reaching an amicable resolution, it may arrange or facilitate such a resolution. Where a complaint is resolved amicably, it will be deemed to have been withdrawn.

Where an amicable resolution cannot be reached, the Commission will take one or more of the actions outlined in subsection (5), including the provision of advice to the complainant, the serving of an enforcement notice (see section 133) on the controller or processor,



conducting an inquiry into the complaint, or dismissing or rejecting the complaint. In each case, the complainant will be informed of the action taken.

Under section 110, the Commission may undertake an inquiry into whether an infringement has occurred, or is occurring, of its own volition or in response to a complaint received by or on behalf of a data subject. For the purposes of any such inquiry, it may exercise its powers under Chapter 4 or carry out an investigation under Chapter 5. Sections 111 and 112 contain provisions concerning decisions of the Commission where an inquiry was conducted on its own volition or in respect of a complaint received respectively.

Section 113 outlines the more complex provisions that apply to cross-border complaints in respect of which the Commission is the lead supervisory authority. In such cases, the Commission is required to prepare a draft decision and consult with other supervisory authorities that, for whatever reason, have an interest in the case. Section 114 deals with the situation arising in other cross-border cases in which the complaint, or part of it, is dismissed or rejected. In the case of both sections 113 and 114, their provisions must be applied in conjunction with the rules applicable to cross-border cases under Articles 60 and 65 of the GDPR.

Section 115 provides that for the purposes of exercising a corrective power in connection with a decision under sections 111, 112 or 113, the Commission may decide to impose an administrative fine or to use any other corrective power set out in Article 58.2 of the GDPR. Section 116 contains provisions concerning the notification of decisions made under these sections. As required by the GDPR, section 117 makes provision for a judicial remedy against a controller or processor.

### Chapter 3

This chapter deals with enforcement of the Directive, as transposed into national law in Part 5. Section 118 contains relevant definitions, while section 119 deals with the lodging of complaints with the Commission. In accordance with Article 55 of the Directive, section 120 makes provision for the representation of data subjects by a not-for-profit body, organisation or association that complies with the conditions outlined in subsection (2).

Sections 121 and 122 contain provisions concerning the handling of complaints by the Commission. These are broadly similar to those set out in sections 108 and 109 in respect of the GDPR. Here also, the Commission may, whether in response to a complaint or of its own volition, carry out an inquiry in order to ascertain whether an infringement has occurred or is occurring. Sections 124 and 125 make provision for Commission decisions, while section 126 makes provision for the notification of Commission decisions.

The corrective powers of the Commission, which are required under Article 47.2 of the Directive, are set out in section 127. Unlike the GDPR, the Directive does not provide for the imposition of administrative fines.

Section 128 provides for a judicial remedy for a data subject where he or she considers that his or her rights have been infringed as a result of the processing of his or her personal data in non-compliance with this Act, or any regulations made under it. It is broadly similar to section 117.

#### Chapter 4

This Chapter contains provisions relevant to the inspection, audit and enforcement powers of the Commission.

Section 129 (Authorised officers) contains general provisions concerning the appointment of authorised officers, while section 130 (Powers of authorised officers) specifies their powers. These are broadly similar to those of inspectors appointed under other legislation of this kind. Where an authorised officer is refused access to premises while exercising his or her powers, he or she may apply to the District Court for a warrant under section 131.

Section 132 (Information notice) provides for the issuing of information notices by the Commission or an authorised officer, requiring a controller or processor to provide information in respect of matters outlined in the notice in the specified format or manner. Section 133 (Enforcement notice) provides that an enforcement notice may require a controller or processor to take such steps as are specified in the notice within such time as may be specified. Under sections 132 and 133, it is an offence for a controller or processor, without reasonable excuse, to fail to comply with an information notice or enforcement notice respectively. These powers correspond broadly with those set out in sections 10 and 12 of the Data Protection Act 1988.

Under section 134, the Commission may, where there is a need to act urgently in order to protect the rights and freedoms of data subjects, apply in a summary manner, on notice to the controller or processor, to the High Court for an order suspending, restricting or prohibiting data processing or the transfer of data to a third country or international organisation. Where urgent, an *ex parte* application may be made and the High Court may make an interim order in such cases. This applies only to urgent cases arising under the GDPR.

Section 135 (Power to require report) provides that the Commission may, for the purposes of proper and effective monitoring of application of the GDPR, require a controller or processor to provide a report to the Commission on any matter about which the Commission could require the provision of information under the GDPR. It is intended that an expert nominated by the controller or processor concerned, and approved by the Commission, will prepare such a report. An expert nominated by the Commission may do so where the controller or processor has failed to nominate an expert or the Commission is not satisfied with the nominated expert.

In advance of requiring production of a report under this section, the Commission will be required to consider whether any other power at its disposal would be more appropriate in the circumstances, as well as the level of resources available to the controller or processor

concerned. This power is broadly based on powers already available to the Central Bank of Ireland under Part 2 of the Central Bank (Supervision and Enforcement) Act 2013.

Under section 136, (Data protection audit), the Commission may carry out audits in order to ascertain whether the practices and procedures of a controller or processor are in compliance with the GDPR and Part 5 of this Act.

#### Chapter 5

Sections 137 to 140 deal with the carrying out of in-depth investigations into possible infringements of the GDPR, this Act or regulations made under it. In accordance with due process standards, it provides for separate investigative and adjudicative stages in an investigation. Section 137 (Investigations) contains general provisions, including the appointment of an authorised officer to undertake the investigation and the notice requirements. Section 138 (Conduct of the investigation under section 137) contains detailed provisions governing conduct of the investigation, including possible administration of an oath and oral hearings. It is an offence under subsection (12) to obstruct such an investigation.

Having completed an investigation, an authorised officer will, in accordance with section 139 (Investigation report), prepare a draft report setting out his or her findings, provide it to the controller or processor concerned for any views they may have, consider any submissions received, and then finalise the report for submission to the Commission. The investigation report will state whether the authorised officer is satisfied that an infringement has occurred or is occurring, and the grounds for that belief. Where an authorised officer has concluded that an infringement has occurred or is occurring, he or she will not make any recommendation, or express any opinion, as to the corrective power that he or she considers ought to be applied in the event that the Commission is also satisfied that an infringement has occurred or is occurring.

On receiving a report, section 140 (Commission to consider investigation report) provides that a Commissioner will consider its contents, including any submissions attached to it. If further information is required, the Commissioner may conduct an oral hearing, seek further submissions from the controller or processor, or require the authorised officer to carry out further investigations.

#### Chapter 6

Sections 141 to 143 contain provisions concerned with the possible imposition of administrative fines under the GDPR. Article 83 of the GDPR provides for the imposition of administrative fines that are effective, proportionate and dissuasive. Such fines may be up to €10 million or €20 million, or up to 2% or 4% of total worldwide annual turnover of a controller or processor during the preceding financial year. When determining whether to impose an administrative fine, and deciding on the amount, due regard must be given to aggravating and mitigating factors set out in paragraph 2 of Article 83.

Section 141 provides that when considering whether to impose an administrative fine, the Commission must act in accordance with Article 83 of the GDPR. Subsection (4) provides that an administrative fine may be imposed on a controller or processor that is a public authority or public body but such a fine shall not exceed €1 million. This lower limit is compliant with paragraph 7 of Article 83 of the GDPR, which provides that it is for each Member State to decide whether, and to what extent, administrative fines may be imposed on public authorities. The limit does not, however, apply where a public authority or public body is acting as an undertaking within the meaning of the Competition Act 2002. For reasons of fairness and equity, all those providing goods and services for gain, i.e. acting as an undertaking, should be subject to the same sanctions regime. Under section 142 (Appeal against administrative fine), a Commission decision to impose an administrative fine may be appealed to the Circuit Court (if the fine does not exceed €75,000) or the High Court within 28 days. On hearing an appeal, the Court may confirm the decision, replace it with another decision that it considers just and appropriate, or annul the decision.

Where no appeal against an administrative fine is lodged under section 142, the Commission will, irrespective of the amount of the fine, make an application in a summary manner to the Circuit Court for confirmation of the decision and the Court shall confirm the decision unless it sees good reason not to do so. The purpose of this confirmation mechanism, based on similar provisions in the Property Services (Regulation) Act 2011, is to ensure that any decision to impose an administrative fine has due regard to fair procedures and constitutional justice.

## Chapter 7

Under section 144 (Unauthorised disclosure by processor), it is an offence for a processor, or an employee or agent of the processor, to disclose personal data being processed on behalf of a controller without the prior authority of the controller, unless the disclosure is required or authorised by or under any enactment, rule of law or order of a court. This offence is carried over from section 21 of the Data Protection Act 1988.

Subsections (1) and (2) of section 145 (Disclosure of personal data obtained without authority) carries over the offence set out in section 22 of the 1988 Act. Subsections (3) and (4) create new offences connected with the selling, or offering for sale, of personal data obtained in contravention of subsection (1).

Section 146 (Offences by directors etc. of bodies corporate) and subsections (1) and (2) of section 147 (Prosecution of summary offences by Commission) replace similar provisions in sections 29 and 30 respectively of the 1988 Act. Subsection (3) of section 147 provides that where a person is convicted of an offence under this Act, the court may, where it is satisfied that there are good reasons for so doing, order the person to pay the costs and expenses incurred by the Commission in relation to the investigation, detection and prosecution of the offence.

## Chapter 8

Under section 148 (General provisions relating to complaints), the Commission may continue to examine the subject matter of a complaint that has been withdrawn, or deemed to have been withdrawn, where it is satisfied that there is good and sufficient reason for so doing. Under subsection (3), where the Commission has doubts concerning the identity of a complainant, it may request additional information in order to confirm his or her identity.

Section 149 (Publication of convictions, sanctions etc.) requires the Commission to publish particulars of convictions under the Act, and any exercise of its powers to impose administrative fines or to order the suspension of transfers of personal data to a third country or international organisation (including Court orders under section 134). It will be a matter for the Commission to decide whether to publish particulars of the exercise of its other corrective powers. It may also publish, if it considers it in the public interest to do so, particulars of any report under section 135 or any report of the Commission of an investigation or audit carried out by it. In doing so, the Commission is required to ensure that publication is done in such a manner that commercially sensitive information relating to a person is not disclosed.

Subsection (1) of section 150 (Right to effective judicial remedy (Part 6)) provides that a controller or processor may appeal against a requirement specified in an information notice or enforcement notice under sections 132 and 133 respectively, and against a notice to provide a report under section 135. Any person, including a data subject, affected by a legally binding decision of the Commission may appeal against it under subsection (5). For the purposes of this section, “legally binding decision” is defined in subsection (12).

Section 151 (Privileged legal material) contains provisions applicable where a controller or processor refuses to produce information to the Commission, or provide access to it, on the grounds that the information contains privileged legal material. In such cases, the Commission or an authorised officer may apply to the High Court for a determination as to whether the information is privileged legal material. Section 152 (Presumptions) specifies the presumptions applicable in any proceedings under the GDPR or this Act. In all cases, such a presumption applies unless the contrary is shown. Section 153 (Expert evidence) makes provision for the admission of expert evidence in court proceedings.

Section 154 (Immunity from suit) provides that civil or criminal proceedings shall not lie in any court against the Commission, Commissioner, authorised officer or member of staff of the Commission in respect of anything said or done in good faith in the course of performance of their functions.

Section 155 deals with the jurisdiction of the Circuit Court, while section 156 provides that proceedings may, at the discretion of the court, be heard otherwise than in public.

## **Part 7 – Miscellaneous matters**

This Part deals with a number of miscellaneous matters. Article 55.3 of the GDPR and Article 45.2 of the Directive provide that the supervisory authority shall not be competent for the supervision of courts when acting in their judicial capacity. For this reason, section 157 provides that a judge assigned for that purpose by the Chief Justice shall be the competent authority for data processing of the courts when acting in their judicial capacity. The task of the assigned judge will include, in particular, promoting awareness of data protection rules among judges and dealing with complaints.

Section 158 restricts, as far as necessary and proportionate, data subject rights and controller obligations in order to protect judicial independence and court proceedings. A panel of three judges nominated by the Chief Justice for that purpose may make such rules as it considers necessary for the purpose of ensuring the effective application of restrictions under this section. Section 159 allocates the task of making rules relating to the processing of personal data in court records to the various Rules Committees already established under the Courts Acts. Section 160 confirms that the processing of personal data is lawful where the processing consists of the publication of a court ruling or decision or a list or schedule of court proceedings or hearings in court proceedings or is necessary for those purposes.

Section 161 makes explicit provision for the making of rules of court for data protection actions referred to in sections 117 and 128. Section 162 restricts data subject rights and controller obligations in so far as these relate to personal data processed for the purpose of seeking, receiving or giving legal advice and to personal data in respect of which a claim of privilege could be made for the purpose of or in the course of legal proceedings.

Section 163 contains provisions that permit the Data Protection Commission to apply to the High Court for a determination as to whether the level of data protection in a third country, a territory or one or more specified sectors within a third country, or an international organisation is adequate. European Commission decisions in respect of the adequacy of data protection are provided for in Article 45.3 of the GDPR and Article 36.3 of the Directive. In such cases, it is likely that the matter would be referred to the Court of Justice in Luxembourg.

## **Part 8 – Amendment of other Acts of the Oireachtas**

This Part contains consequential amendments to other Acts. These amendments are necessary in order to replace existing cross-references to the Data Protection Act 1988 with references to the Regulation and/or Part 5 of this Act.

Schedule 1 contains a listing of revoked Statutory Instruments; Schedule 2 contains provisions in relation to the Data Protection Commission established under Part 2; Schedule 3 contains provisions applicable to oral hearings conducted by authorised officers under Part 6.

September 2018