General Scheme of Data Protection Bill (May 2017)

PART 1
1 – Citation and commencement
2 – Interpretation
3 – Expenses
4 – Regulations
5 – Repeals

PART 2
6 – Establishment Day
7 – Data Protection Commission
8 – Functions
9 – Membership of commission
10 – Staff of the commission
11 – Membership etc., of Dáil, Seanad or European Parliament
12 – Financial control
13 – Attendance of Commissioner before Oireachtas Committee
14 – Prohibition on unauthorised disclosure of information
15 – Transfer of property, preservation of contracts, pending proceedings and saving for certain acts.

PART 3
16 – Child’s consent in relation to information society services
17 – Processing of special categories of personal data for reasons of substantial public interest
18 – Processing of special categories of personal data
19 – Processing of personal data relating to criminal convictions and offences
20 – Restrictions on exercise of data subject rights and controller obligations
21 – Designation of data protection officer
22 – Limitation on transfer of personal data outside the EU
23 – Imposition of administrative fines on public authorities and bodies
24 – Data processing and freedom of expression and information
25 – Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
PART 4

Chapter 1

26 – Interpretation
27 – Application of this Part
28 – Collection, processing, keeping and use of personal data
29 – Security measures for personal data
30 – Data quality
31 – Processing of sensitive personal data

Chapter 2

32 – Restriction on automated individual decision making
33 – Right to information
34 – Right of access
35 – Right to rectification, erasure or restriction of processing
36 – Communication with data subjects
37 – Restrictions
38 – Indirect exercise of rights and verification by supervisory authority
39 – Data subject rights in criminal investigations and proceedings

Chapter 3

40 – Obligations of data controller
41 – Data protection by design and default
42 – Processor
43 – Records of data processing activities
44 – Data logging obligations
45 – Cooperation with the commission
46 – Data protection impact assessment and prior consultation with Commission
47 – Security of processing
48 – Notification of personal data breach to Commission
49 – Communication of personal data breach to data subject
50 – Designation of data protection officer

Chapter 4

51 – Transfers of personal data to third countries and international organisations
52 – Transfers subject to appropriate safeguards
53 – Derogations for specific situations
54 – Transfers to recipients in third countries

Chapter 5
55 – Right to lodge a complaint with Commission
56 – Right to effective judicial remedy against Commissioner
57 – Representation of data subject
58 – Right to compensation

Chapter 6
59 – Supervisory authority
60 – Tasks of the Commission
61 – Powers of the Commission
62 – Mutual assistance

PART 5
Chapter 1
63 – Interpretation
64 – Service of notice

Chapter 2
65 – Data subject complaints
66 – Investigation and audit
67 – Authorised officers
68 – Search warrants
69 – Power to require information
70 – Power to enforce
71 – Right to an effective judicial remedy
72 – Exceptional circumstances in which application may be made to the High Court
73 – Power to require report

Chapter 3
74 – Investigations
75 – Power of investigation
76 – Report of authorised officer

Chapter 4
77 – Action arising from investigation report
78 – Cooperation and consistency mechanism
79 – Appeal against administrative fine
80 – Circuit Court to confirm decision to impose administrative fine
81 – Unauthorised disclosure by processor
82 – Disclosure of personal data obtained without authority
83 – Offences by directors etc. of bodies corporate
84 – Prosecution of summary offences by Commission
85 – Publication of convictions, sanctions etc.

Chapter 5
86 – Privileged legal material
87 – Presumptions
88 – Expert evidence
89 – Immunity from suit

PART 6
90 – Supervisory authority for courts acting in judicial capacity
91 – Judicial remedy
92 – Rules of court
93 – Legal privilege
94 – Amendment of section 33AK of Central Bank Act 1943
95 – Application to refer case to the CJEU

Part 7

Schedule
Provisions applicable to oral hearing conducted by an authorised officer under Head 75
Part 1

General Provisions

Head 1 – Citation and commencement

Provide that:

1. This Act may be cited as the Data Protection Act 2017.

2. This Act shall come into operation on such day or days as the Minister may appoint by order or orders either generally or with reference to any particular Part or purpose, and different days may be so appointed for different Parts and different purposes.

Explanatory Notes

This is a standard provision.
Head 2: Interpretation

Provide that:

1. In this Act, unless the context otherwise requires—

“appropriate authority” has the meaning assigned to it in the Civil Service Regulation Acts 1956 to 2005; (new definition inserted by 2005 Act);

“Commission” has the meaning given to it in Head 7;

“Directive” means DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA;

“Regulation” means REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

“Minister” means the Minister for Justice and Equality;

“relevant Minister” means that Minister of the Government on whom functions stand conferred or who has general responsibility in respect of or connected to the matter concerned.

2. (a) An appropriate authority, being a controller or a processor, may, as respects all or part of the personal data processed by the authority, designate a civil servant in relation to whom it is the appropriate authority to be a controller or a processor and, while the designation is in force—

(i) the civil servant so designated shall be deemed, for the purposes of this Act, to be a controller or, as the case may be, a processor, and
(ii) this Act shall not apply to the authority, as respects the personal data concerned.

(b) Without prejudice to paragraph (a), the Minister for Defence may, as respects all or part of the personal data processed by him or her in relation to the Defence Forces, designate an officer of the Permanent Defence Force who holds a commissioned rank to be a controller or a processor and, while the designation is in force—

(i) the officer so designated shall be deemed, for the purposes of this Act, to be a controller or, as the case may be, a processor, and

(ii) this Act shall not apply to the Minister for Defence, as respects the personal data concerned.

(c) For the purposes of this Act, as respects any personal data—

(i) where a designation by the relevant appropriate authority under paragraph (a) of this subsection is not in force, a civil servant in relation to whom that authority is the appropriate authority shall be deemed to be its employee and, where such a designation is in force, such a civil servant (other than the civil servant the subject of the designation) shall be deemed to be an employee of the last mentioned civil servant,

(ii) where a designation under paragraph (b) of this subsection is not in force, a member of the Defence Forces shall be deemed to be an employee of the Minister for Defence and, where such a designation is in force, such a member (other than the officer the subject of the designation) shall be deemed to be an employee of that officer, and

(iii) a member of the Garda Síochána (other than the Commissioner of the Garda Síochána) shall be deemed to be an employee of the said Commissioner.

Explanatory notes

Subhead 1 contains relevant definitions. Subhead 2 reproduces section 1(3) of the Data Protection Act 1988; it permits Ministers and other “appropriate authorities” (defined in section 6 of the 1956 Act, as substituted in the 2005 Act) who are controllers to designate one of more of their civil servants to be controllers or processors for the purposes of the legislation. It does not apply to the wider public sector.
Head 3: Expenses

Provide that:

The expenses incurred in respect of the Commission under this Act and expenses incurred by any Minister in the administration of this Act shall, to such extent as may be sanctioned by the Minister for Public Expenditure and Reform, be paid out of moneys provided by the Oireachtas.

Explanatory notes

This is a standard provision in legislation of this kind.
Head 4: Regulations

Provide that:
A regulation made under this Act shall be laid before each House of the Oireachtas as soon as may be after it is made and, if a resolution annulling the order or regulation is passed by either such House within the next 21 days on which that House has sat after the order or regulation is laid before it, the order or regulation shall be annulled accordingly, but without prejudice to the validity of anything previously done thereunder.

Explanatory notes
This is a standard provision. Several regulation-making powers are included, especially in Part 3. This provision does not apply to orders under Head 1 or Head 6.
Head 5: Repeals

Provide that:

[ ]

Explanatory notes

The Data Protection Acts 1988 and 2003 will be largely superseded by provisions in the GDPR and Part 4 of this Bill which gives effect in national law to the law enforcement Directive.

Article 2 (Material scope) of the GDPR provides that its provisions do not apply to processing of personal data in the course of activities that lie outside the scope of EU law (e.g. national security) and those falling under the common foreign and security policy. Discussions are continuing on the question of whether and, if so, to what extent, provisions in the 1988 and 2003 Acts may need to be retained.

It is clear that some statutory instruments made under regulation-making powers in the Acts of 1988 and 2003 will need to be revoked, e.g. those dealing with fees (registration fees and access fees are abolished by the GDPR) while other may be retained. Work is ongoing in relation to this matter.

This Head will be completed during the drafting process.
Part 2

Data Protection Commission

Head 6 – Establishment day

Provide that:

The Minister shall, by order, appoint a day to be the establishment day for the purposes of this Part.

Explanatory notes

Head 7 makes provision for an ‘establishment day’ order which would establish the Data Protection Commission to replace the Data Protection Commissioner. This would permit, if justified by an increased future workload, the appointment of more than one Commissioner. In such a scenario, one of them would be appointed as chairperson.
Head 7 – Data Protection Commission

Provide that:

1. On the establishment day there shall stand established a body to be known as the Data Protection Commission or, in the Irish language, An Coimisiún um Cosanta Sonrai (in this Act referred to as the “Commission”), which shall perform the functions conferred on it by or under the Regulation and this Act.

2. The Commission—
   (a) shall be a body corporate with perpetual succession and an official seal,
   (b) may sue and be sued in its corporate name, and
   (c) may acquire, hold and dispose of land or an interest in land or any other property.

3. The seal of the Commission may be authenticated by the signature of—
   (a) a Commissioner, or
   (b) a member of staff of the Commission so authorised.

4. Judicial notice shall be taken of the seal of the Commission and in any proceedings, a document purporting to be a document made or issued by, and to be sealed with the seal of, the Commission and any copy so sealed of such a document is admissible, without further proof, as evidence of the document and the matters mentioned in it.

5. Any contract or instrument which, if entered into or executed by an individual, would not require to be under seal may be entered into or executed on behalf of the Commission by a member of staff generally or specially authorised for that purpose.

Explanatory notes
This Head incorporates paragraph 1 of the Second Schedule to the Data Protection Act 1988 and includes a number of additional standard provisions.
Head 8 – Functions

Provide that:

1. The Commission shall be completely independent in the performance of its tasks and exercise of its powers under the Regulation and this Act.

2. The functions of the Commission are—
   (a) to act as the supervisory authority referred to in Article 51 of the Regulation and thereby to perform the tasks and exercise the powers conferred by Articles 57 and 58 respectively;
   
   (b) to act as the supervisory authority referred to in Article 41 of the Directive and thereby to perform the tasks and exercise the powers conferred by Heads 60 and 61 of this Act respectively,
   
   (c) to perform such other functions in relation to data protection that the Minister may confer on it by regulations for the purpose of enabling the Government to give effect to any international obligation of the State.

3. (a) The lawfulness of the processing of personal data (including their transmission to the Central Unit of Eurodac established pursuant to the Regulation) in accordance with the Regulation shall be monitored by the Commission.
   
   (b) In paragraph (a), the Regulation means Regulation (EU) of the European Parliament and the Council on the establishment of Eurodac for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes

4. The Commission shall disseminate, to such extent and in such manner as it considers appropriate, information in relation to the tasks performed and powers exercised by it.
5. The Commission may do anything which it considers necessary or expedient to enable it to perform its tasks and exercise its powers.

6. References in any enactment to the Data Protection Commissioner are deleted and references to the Data Protection Commission inserted.

7. Subject to the Regulation and this Act, internal procedures may be prescribed by means of regulations made by the Commission following consultation with the Minister.

Explanatory notes
The primary function of the Commission will be to act as the supervisory authority for the purposes of the GDPR and the law enforcement Directive (transposed in this legislation). Subhead 2(c) reproduces section 9(1D) of the 1988 Act (as amended).

Subhead 3 reproduces section 9(1A) of the 1988 Act as inserted by the 2003 Act. Subheads 4 and 5 are standard provisions.

The Commissioner has been given statutory functions under other enactments and regulations. For example, section 19 of the Credit Reporting Act 2013 refers to the Commissioner. The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 made by the Minister for Communications, Energy and Natural Resources to give effect to Directive 2002/58/EC (as amended in 2006 and 2009) designates the Commissioner as supervisory authority for its purposes.

A ‘conversion’ provision on the lines of subhead 6 which would convert all references to the Commissioner into references to the Commission will be required; this may not be sufficient in all cases, however, and transitional provisions may be required in order to ensure a smooth transition from Commissioner to Commission.

Subheads 7 would allow, where appropriate, internal procedures of the Commission to be prescribed in regulations. It would, for example, permit the making of internal rules for the handling of complaints “to the extent appropriate” as referred to in Article 57.1(f).
Head 9 – Membership of Commission

Provide that:

1. The Commission shall consist of at least one member and not more than 3 members.

2. Each member of the Commission shall be known as a Commissioner for Data Protection and is in this Act referred to as a “Commissioner”.

3. A Commissioner shall be appointed by the Government on the recommendation of the Public Appointments Service.

4. In recommending a candidate for appointment as Commissioner, the Public Appointments Service shall have regard to the need for him or her to have the qualifications, experience and skills, notably in the area of data protection, required in order for the Commission effectively to perform its tasks and exercise its powers under the Regulation and this Act.

5. (a) Where there is more than one Commissioner, the Minister shall appoint one of them to be the chairperson of the Commission (in this section referred to as “the Chairperson”).

(b) The Minister shall, when appointing the Chairperson, with the consent of the Minister for Public Expenditure and Reform, fix the terms and conditions, including remuneration, of the Chairperson.

6. A Commissioner appointed in accordance with subhead 3 shall be appointed on a full-time basis for a period of not less than 4 years and not more than 5 years, and may be reappointed for a further period not exceeding 5 years.

7. The Chairperson shall have a casting vote in the case of decisions to be taken by the Commission in the event of a tied vote.

8. Notwithstanding subhead 3, the person who is the Data Protection Commissioner immediately before the establishment day shall be a Commissioner for Data Protection and shall hold that office
subject to terms and conditions which are not less favourable than those of his or her appointment as Data Protection Commissioner.

9. A Commissioner may resign by giving notice in writing to the Minister of his or her intention to resign and any such resignation shall take effect as of the date upon which the Minister shall have received notice of the resignation.

Explanatory notes
The anticipated additional workload arising from the GDPR and this Act, arising especially in the context of the GDPR from operation of the consistency mechanism (One-Stop-Shop), requires an examination of the need to make provision for the appointment of additional Commissioners. This Head draws inspiration from the legislation establishing the Commission for Communications Regulation (Communications Regulation Act 2002).

It provides for a minimum of 1 member of the Commission and for a maximum of 3 members (one of whom would be Chairperson).

The possibility of stringent sanctions, including large administrative fines, arising from the investigation of complaints or the conduct of data protection audits, means that rigorous procedural safeguards and due process standards must be maintained in order to withstand likely court challenges. This will require separation of the investigative and adjudicative processes within the Commission and will impose a significant additional workload on the Commissioner. Depending on the circumstances of a case, e.g. if imposition of a large administrative fine is likely, the Commissioner may need to hold an oral hearing. There is a likelihood of resource intensive ‘One-Stop-Shop’ cases arising in this jurisdiction in light of the large number of data processing companies based here (including those servicing data subjects across the EU such as Facebook, Linked-In etc.).

As regards dismissal, consideration will be given to inclusion of provisions such as the following (based on section 18 of the Communication Regulation Act 2002) during the drafting stage in order to respect Article 53.4:

A Commissioner may be removed from office by the Government—
(a) if, in its opinion, the Commissioner has become incapable through ill health or otherwise of effectively performing his or her duties, or
(b) for reasons of serious misconduct.

- In removing a Commissioner, the Government shall give a statement of the reason or reasons for the removal to the Commissioner and the statement of reasons shall be laid before each House of the Oireachtas.

It will be important to ensure that any such provisions do not impinge on the independence of the Commission.
Head 10 – Staff of the Commission

Provide that:

1. Subject to subhead 3 [and Head 9], the Commission may appoint such number of persons to be members of its staff as it may determine.

2. Subject to subhead 3, the Commission shall determine the grades of members of its staff and the numbers in each grade.

3. A determination of the Commission under subhead 1 or 2 is subject to the approval of the Minister and the consent of the Minister for Public Expenditure and Reform.

4. The Minister may delegate to the Commission the powers exercisable by him or her under the Public Service Management (Recruitment and Appointments) Act 2004, and the Civil Service Regulation Acts 1956 and 1958, as the appropriate authority in relation to members of the staff of the Commission and, if he or she does so, then so long as the delegation remains in force—
   (a) those powers shall, in lieu of being exercisable by the Minister, be exercisable by the Commission, and

   (b) the Commission shall, in lieu of the Minister, be for the purposes of this Act the appropriate authority in relation to members of the staff of the Commission.

5. The functions of the Commission may be performed on its behalf by any member or members of its staff who is or are so authorised.

6. A member of staff of the Commission who performs any of its functions is presumed in any proceedings to have been authorised to do so on its behalf, unless the contrary is shown.

7. Members of the staff of the Commission are civil servants in the Civil Service of the Government.

8. The Commission is the appropriate authority (within the meaning of the Civil Service Commissioners Act 1956 and the Civil Service Regulation Acts 1956 to 2005) in relation to its staff.
9. Every person who immediately before the establishment day was a member of the staff of the Data Protection Commissioner shall become a member of the staff of the Commission on that day.

Explanatory notes
This Head provides for staffing of the Commission. Under subhead 9, existing staff would become staff of the Commission.
Head 11 – Membership etc., of Dail, Seanad or European Parliament

Provide that:

1. A Commissioner ceases to hold office on—
   (a) accepting nomination as a member of Seanad Eireann,
   (b) being elected as a member of either House of the Oireachtas or to be a representative in the European Parliament, or
   (c) being regarded under Part XIII of the Second Schedule to the European Parliament Elections Act 1997 as having been elected to that Parliament.

(2) A person who is for the time being—
   (a) entitled under the Standing Orders of either House of the Oireachtas to sit therein,
   (b) a member of the European Parliament, or
   (c) entitled under the standing orders of a local authority to sit therein,

is, while so entitled or is such a member, disqualified from holding the office of Commissioner.

Explanatory notes
This is a standard provision (already in the Second Schedule to 1988 Act).
Head 12 – Financial control

Provide that:

[ ]

Explanatory notes
Article 52.6 of the GDPR provides as follows:

“Each Member State shall ensure that each supervisory authority [note: they are allowed to have more than one] is subject to financial control which does not affect its independence and that it has separate, public budgets, which may be part of the overall state or national budget.”

In consultation with the Department of Public Expenditure and Reform, the adequacy of financial control arrangements currently applicable to the Data Protection Commissioner will be examined during the drafting process and the question of whether a separate Vote and Accounting Officer role for the Commission would be appropriate in order to comply with the independence requirement will be considered in that context.
Head 13 – Attendance of Commissioner before Oireachtas Committee

Provide that:

1. The Commissioner or, in the event of more than one Commissioner, the Chairperson shall, at the request in writing of a committee of the Oireachtas, attend before it to give account for the general administration of the Commission and report on the performance of its functions.

2. In this Head, “committee of the Oireachtas” means a committee appointed by either House of the Oireachtas or jointly by both Houses of the Oireachtas (except the Committee on Members’ Interests of Dail Éireann or the Committee on Members’ Interests of Seanad Éireann) or a subcommittee of a committee so appointed.

Explanatory notes
Article 52.6 specifies that member States shall ensure that each supervisory authority is subject to financial control which does not affect its independence. Accountability to an Oireachtas Committee, rather than to the Minister and Department, will serve to underpin the functional independence of the Commission while ensuring adequate financial control.
Head 14 – Prohibition on unauthorised disclosure of information

Provide that:

1. The disclosure of information that comes into the possession of the Commission by virtue of the performance of its tasks and exercise of its powers under the Regulation and this Act is prohibited.

2. Subhead (1) shall not apply to—
   (a) a communication made by a Commissioner, authorised officer or member of staff in the performance of any of his or her functions under the Regulation or this Act, being a communication the making of which was necessary for the performance by the Commissioner, authorised officer or member of staff of any such function,

   (b) disclosure of information in a report of the Commission or for the purpose of legal proceedings under this Act or pursuant to an order of a court of competent jurisdiction for the purposes of any proceedings in that court,

   (c) disclosure by a Commissioner, authorised officer or member of staff to any member of the Garda Síochána of information which, in the opinion of the Commissioner, authorised officer or member of staff, may relate to the commission of an offence (whether an offence under this Act or not),

   (d) disclosure of information required or permitted by law or an enactment, whether under the Regulation, this Act or otherwise, including such disclosure to the supervisory authority of another Member State, or

   (e) disclosure of information to a public authority, whether in the State or otherwise, for the purpose of facilitating cooperation between the Commission and such authority in the performance of their respective functions.
3. A person who contravenes subhead 1 shall be guilty of an offence and shall be liable on summary conviction to a class A fine.

4. A person who suffers loss or harm as a result of a contravention of subhead 1 shall be entitled to bring proceedings against a person referred to in subhead 5 who has been convicted of an offence under subhead 3 in any court of competent jurisdiction seeking the following reliefs in respect of that loss or harm—
   (a) injunction or declaration
   (b) damages.

5. The person referred to in subhead 4 is—
   (a) if the person who contravened subhead (1) is other than a Commissioner, an authorised officer or member of staff, that person,
   (b) if the person who contravened subhead (1), is a Commissioner, an authorised officer or member of staff and the relief sought, or to the extent that the relief sought, in the proceedings is—
      (i) relief referred to in subhead (4)(a), that person,
      (ii) relief referred to in subhead (4)(b), the Commission.

6. An action under subhead 4 is an action founded on tort.

**Explanatory notes**

Article 49.2 of the Regulation contains the following provision:

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, this duty of professional secrecy shall in particular apply to reporting by individuals of infringements of this Regulation.

This Head will replace paragraph 10 of the Second Schedule to the 1988 Act.
Head 15 – Transfer of property, preservation of contracts, pending proceedings and saving for certain acts

Provide that:

1. (a) On the establishment day, property other than land that immediately before that day was being used in connection with a function of the Data Protection Commissioner stands vested in the Commission without any assignment.

(b) In subhead (a), “property” includes any chose in action arising in connection with a function of the Data Protection Commissioner corresponding to a function of the Commission.

2. A chose in action vested in the Data Protection Commissioner under subhead 1 may, on and after the establishment day, be sued on, recovered or enforced by or against the Commission in its own name, and the Commission or the Minister need not give notice of the vesting to any person bound by the chose in action.

3. On the establishment day, documents and records that were held by the Data Protection Commissioner immediately before that day stand vested in the Commission.

4. Any contract, agreement or arrangement made between the Data Protection Commissioner and any other person and in force immediately before the establishment day—

(a) continues in force on or after that day, and

(b) has effect as if the name of the Commission were substituted in the contract, agreement or arrangement for the Data Protection Commissioner.

5. If, immediately before the establishment day, any proceedings are pending in any court or tribunal to which the Data Protection Commissioner is a party, the name of the Commission is substituted in the proceedings, and the proceedings do not abate by reason of the substitution.

6. Nothing in this Act affects the validity of any act done or in the course of being done before the establishment day by or on behalf of the Data Protection Commissioner and any such act, if and in
so far as it was operative immediately before that day, has effect on and after that day as if it had been done by or on behalf of the Commission.

Explanatory notes
This Head contains provisions which are intended to facilitate a smooth transition from the Data Protection Commissioner to the Commission.
Part 3 – Heads to give further effect to GDPR

1. The GDPR provides limited flexibility for Member States to enact national law to adapt certain of its provisions to the needs of their legal systems and public sectors. This Part contains Heads which seek to give further effect to Articles 8, 9, 10, 23, 37, 49, 83, 85, and 89. Ancillary provisions to govern the performance of tasks and exercise of powers by the Data Protection Commission (in particular, paragraphs 4, 5 and 6 of Article 58) are set out in Part 5 of the Bill. Provisions in relation to the judicial remedies referred to in Articles 77, 78 and 79 are in Part 6. Court rules will be required in due course.

2. Except where indicated otherwise, the definitions of terms used in these Heads are those set out in Article 4 of the Regulation. Recital (8) restricts the extent to which elements of the Regulation text may be incorporated into national law.

3. As regards interpretation and application of the Regulation, the European Data Protection Board established by Article 70 will play a key role in future (the current Article 29 Committee is already preparing for this). The Board is tasked with ensuring consistent and correct application of the Regulation and will, for this purpose, issue guidelines, recommendations and best practices. It is likely that these will prove very influential in the context of data protection proceedings coming before the Court of Justice.

4. **Head 16**: It will specify a ‘digital age of consent’ for the purposes of Article 8. A consultation process on the appropriate age threshold has been completed and the results will be submitted to Government for a decision in due course.

5. **Head 17**: Paragraph 1 of Article 9 prohibits the processing of special categories of personal data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation) except where permitted under paragraph 2. Under subparagraph (g), the processing of such sensitive data may be processed where “necessary for reasons of substantial interest”. This Head permits the making of regulations to underpin such processing. A similar provision already exists in Article 2B(1)(xi) of the Data Protection Act 1988 (as amended).

6. **Head 18**: Subheads 1 to 4 seek to give effect to the margin of flexibility afforded under Article 9.2 (b), (h), (i) and (j) and paragraph 4. Subhead 5 provides for the processing of biometric data for the purposes of identification and for security purposes, subject to appropriate safeguards.

7. **Head 19**: Article 10 of the Regulation provides that the processing of personal data relating to criminal convictions and offences or related security measures may take place, subject to
appropriate safeguards for the rights and freedoms of data subjects, under the control of official authority or where authorised under Union of Member State law. Existing statutes may already provide a sufficient legal basis for processing such data, e.g. company law provisions in respect of Company Registration Office and the Office of the Director of Corporate Enforcement. However, this Head seeks to provide a more general basis for such processing, subject to appropriate safeguards.

8. **Head 20:** Article 23 of the Regulation permits limited restrictions on controller/processor obligations and the exercise of data subject rights in Chapter III in so far as such restrictions are necessary to safeguard important objectives of general public interests of the Union or a Member State. Such restrictions are permitted subject to 3 conditions:
   a. a legislative measure is required;
   b. it must be proportionate (“necessary and proportionate measure in a democratic society”)
   c. the essence of the right to data protection must be respected.

9. Some statutes would appear to contain at least some of the requirements of Article 23, e.g. Credit Reporting Act 2013 (credit rating); Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (money laundering). While it would be desirable for all Departments to consider the need for specific amendments to primary legislation governing their own activities and those of public authorities and bodies operating under their aegis, this Head is intended to permit the Minister or relevant Ministers, as the case may be, to make regulations for their own areas of activity and those of their agencies.

10. The list of “important objectives of general public interest” in subhead 2 takes account of those set out in Article 23.1. The list is not closed and the Head contains a mechanism for recognising additional objectives of general public interest.

11. Subhead 3 list the matters which, according to Article 23.2, should be considered “at least, where relevant” in the making of regulations.

12. **Head 21:** Article 37.1 of the Regulation requires the appointment of a data protection officer in certain cases, including in the case of public authorities and bodies. However, paragraph 4 provides a margin of flexibility for Member States by allowing them to enact national law which would require the appointment of data protection officers in other cases. This Head seeks to create a regulation-making power so that the flexibility may be availed of, if necessary and to the extent justified, in future.

13. **Head 22:** In the absence of an adequacy decision under Article 45, paragraph 5 of Article 49 gives Member States a margin of flexibility to restrict, for important public interest reasons, the transfer of specific categories of personal data to a third country or an international
organisation. Creation of a regulation-making power will facilitate the possibility of a speedy response to the emergence of such a risk.

14. **Head 23:** Article 83 provides for the imposition of substantial fines on data controllers or data processors for infringements of its provisions. However, paragraph 7 permits flexibility in the case of public authorities and bodies. In order to avoid the risk of competitive distortions and accusations of inequitable treatment, this Head provides that administrative fines may be imposed on a public authority or body in respect of an infringement arising from its activity as an undertaking (i.e. providing goods or services for gain - not necessarily for profit - in a market).

15. **Head 24:** This Head seeks to give effect to Article 85 which provides that it shall be for member State law to reconcile the right to protection of personal data with the right to freedom of expression and information. Current law in this regard is set out in section 22A of the Data Protection Act 1988 (inserted by the Data Protection (Amendment) Act 2003) which gives effect to Article 9 (Processing of personal data and freedom of information) of the 1995 Data Protection Directive.

16. **Head 25:** This Head seeks to give effect to Article 89 of the Regulation which provides for derogations, subject to certain conditions, from specific data subject rights in Chapter III of the Regulation for ‘privileged purposes’ (i.e. processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes). A legal basis for the processing of special categories of personal data for these purposes is provided in Head 18.

17. **Article 6.2 and 3** of the Regulation allows Member States to adapt application of the rules of the Regulation to their public sectors. This will be a matter for sectoral legislation. **Article 88** allows member States to provide more specific rules in the employment context.
Head 16: Child’s consent in relation to information society services [Article 8]

Provide that

For the purpose of Article 8 of the Regulation, [ ] years shall be the age below which data processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Explanatory notes

A separate Government decision will be sought on “the digital age of consent” for the purposes of this Head.

Article 8 of the Regulation (below) permits Member States to specify an age which is lower than 16 years:

1. Where point (a) of Article 6(1) applies [i.e. processing based on data subject consent], in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 4(25) reads as follows:

“information society service” means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Councils;

Head 17: Processing of special categories of personal data for reasons of substantial public interest [Article 9.2(g)]

Provide that:

Pursuant to Article 9.2(g) of the Regulation, the processing of special categories of personal data may be authorised by regulations that are made by—

(a) the Minister following consultation with a relevant Minister (if any) and the Commission, or

(b) by a relevant Minister following consultation with the Minister and the Commission,

and are made for reasons of substantial public interest on condition that such regulations—

(i) contain suitable and specific measures to safeguard the fundamental rights and interests of the data subject, and

(ii) respect the essence of the right to the protection of personal data and are necessary and proportionate to the aim pursued.

Explanatory notes

Paragraph 1 of Article 9 of the Regulation prohibits the processing of special categories of personal data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) except where permitted under paragraph 2.

Paragraph 2(g) of Article 9 permits, subject to conditions, the processing of such special categories of personal data where “necessary for reasons of substantial public interest”. This Head permits the making of regulations to underpin such processing. A similar provision is found in Article 2B(1)(xi) of the 1988 Act, as amended by the 2003 Act.
Head 18: Processing of special categories of personal data [Article 9.2 (b), (h), (i) and (j) and 4]

Provide that:

1. Subject to suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject, processing of special categories of personal data is permitted where necessary for—
   a. purposes of preventive or occupational medicine,
   b. assessment of the working capacity of an employee,
   c. medical diagnosis,
   d. provision of health or social care or treatment,
   e. management of health and social care systems and services,
   f. public interest reasons in the area of public health, or
   g. pursuant to a contract with a health professional. [Article 9.2(h)]

2. Without prejudice to the generality of subhead 1(f), processing of personal data for reasons of public interest in the area of public health includes—
   a. protecting against serious cross-border threats to health,
   b. ensuring high standards of quality and safety of health care and of medicinal products and medical devices. [Article 9.2(i)]

3. Subject to suitable and specific measures to safeguard the fundamental rights and interests of the data subject, processing of special categories of personal data is permitted in accordance with Head 25 where necessary and proportionate for—
   a. archiving purposes in the public interest,
   b. scientific or historical research purposes,
   c. statistical purposes. [Article 9.2(j)]

4. Subject to suitable and specific measures to safeguard the fundamental rights and the interests of the data subject, processing of special categories of personal data is permitted where necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law. [Article 9.2(b)]
5. Subject to suitable and specific measures to safeguard the fundamental rights and the interests of the data subject, biometric data may be processed for identification and security purposes.

Explanatory notes
Subheads 1, 2, 3 and 4 seek to give effect to the margin of flexibility afforded under Article 9.2 (i.e. special categories of personal data).

There is continuing uncertainty as to the extent to which the “suitable and specific safeguards” referred to in Article 9 are intended to be additional or complementary to data controller obligations already required under Articles 24, 25 and 32. The possibility of including a ‘toolbox’ of possible safeguards in a new subhead will be explored during drafting.

Article 9.4 permits Member States to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data and health data. This could permit the maintenance of limitations in sectoral statutes, e.g. prohibition on processing of genetic data set out in the Disability Act 2005. Subhead 5 provides for the processing of biometric data for the purposes of identification and for security purposes, subject to appropriate safeguards.
Head 19: Processing of personal data relating to criminal convictions and offences (Article 10)

Provide that:

1. Subject to Article 6.1 and subhead 2, personal data relating to criminal convictions and offences or related security measures may be processed by a controller or processor for one or more of the following specific purposes:
   
   (a) processing is necessary for the assessment of risk or prevention of fraud;

   (b) processing is necessary for purposes of exercising a regulatory, authorising or licensing function or determining eligibility for benefits or services;

   (c) processing is necessary to protect the public against harm arising from dishonesty, malpractice, breaches of ethics or other improper conduct by, or the unfitness or incompetence of, persons authorised to carry on a profession or other activity;

   (d) processing is necessary for the establishment, defence or enforcement of civil law claims;

   (e) processing is necessary for enforcement actions, whether in the State or otherwise, aimed at preventing, detecting or investigating breaches of EU or national law that are subject to civil or administrative sanctions;

   (f) processing is necessary for ensuring network and information system security, and the prevention of attacks on and damage to computer and electronic communications systems;

   (g) processing is necessary for the rehabilitation or reintegration of offenders;

   (h) processing is necessary for exercising the right to freedom of expression and information;

   (i) processing is necessary to protect the safety and well-being of children and vulnerable adults or to protect a data subject or the rights and freedoms of others.

2. Processing of personal data for purposes referred to in subhead 1 shall be subject to appropriate safeguards for the rights and freedoms of data subjects.

3. In this Head, “conviction”, in relation to an individual, means the conviction by a court or equivalent tribunal of the individual of an offence or, in the case of an appeal (whether against
conviction or sentence, or both), the final determination by a court or tribunal of the appeal, or the withdrawal of the appeal.

4. This Head is without prejudice to operation of the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016.

**Explanatory Notes**
This Head seeks to give effect to Article 10 of GDPR.

**Subhead 1**
Where a legal ground for processing exists under Article 6.1, this Head will permit the processing of personal data relating to criminal conviction data, subject to appropriate safeguards, for the various purposes outlined in (a) to (i). The nature of these safeguards will be discussed during drafting.

**Subhead 2**
Article 10 requires that appropriate safeguards must be put in place for the purposes of processing this type of data. The possibility of including a ‘toolbox’ of possible safeguards in a new subhead will be explored during drafting.

**Subhead 3**
This is a short definition of “conviction” and may need to be expanded; there is no definition of criminal conviction in the GDPR.

**Subhead 4**
National law permits certain minor offences to be disregarded after a period of time (7 years) provided there have been no further convictions.
Head 20 – Restrictions on exercise of data subject rights (Article 23)

Provide that:

1. The scope of rights and obligations provided for in Articles 12 to 22 and Article 34 of the Regulation (as well as Article 5 in so far as its provisions correspond to such rights and obligations), may be restricted by means of regulations made by—

   (a) the Minister following consultation with a relevant Minister and the Commission, or

   (b) a relevant Minister following consultation with the Minister and the Commission,

in order to safeguard important objectives of general public interest referred to in subhead 2, provided such restriction respects the essence of the right to the protection of personal data and is a necessary and proportionate measure in a democratic society.

2. Important objectives of general public interest include—

   (a) safeguarding national security, defence and the international relations of the State;

   (b) preventing threats to public security and public safety;

   (c) avoiding obstructions to an official or legal inquiry, investigation or process, including any proceedings pending or due before a court, tribunal of inquiry or commission of investigation;

   (d) preventing, detecting, investigating or prosecuting criminal or disciplinary offences and the execution of penalties;

   (e) preventing, detecting, investigating or prosecuting breaches of ethics for regulated professions,

   (f) preventing, detecting and investigating, whether in the State or otherwise, breaches of law which are subject to civil or administrative sanctions, and enforcing such sanctions;

   (g) the identification of assets which derive or are suspected to derive from criminal conduct and the taking of appropriate action to deprive or deny persons of the assets or the benefit of such assets as well any investigation or other preparatory work in relation to any related proceedings;

   (h) orderly regulation of asylum and immigration matters;
(i) administering any tax, duty or other moneys owed or payable to the State, a local authority or other public authority or body;

(j) safeguarding economic or financial interests of the Union or the State, including monetary, budgetary and taxation matters;

(k) safeguarding monetary policy, the smooth operation of payment systems, the resolution of regulated financial service providers, the operations of deposit-guarantee scheme, the protection of consumers, and the proper and effective regulation of financial service providers;

(l) protecting members of the public against—
   (i) financial loss or detriment due to dishonesty, malpractice or other improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate or other entities,
   (ii) financial loss due to the conduct of persons who have been adjudicated bankrupt;

(m) protecting members of the public against harm arising from dishonesty, malpractice, breaches of ethics or other improper conduct by, or the unfitness or incompetence of, persons authorised to carry on a profession or other activity;

(n) protecting—
   (i) the health, safety, dignity and well-being of individuals at work against risks arising out of or in connection with their employment, and
   (ii) members of the public against discrimination or unfair treatment in the provision of goods and/or services to them;

(o) protecting the rights and freedoms of individuals, including their safety and well-being;

(p) the protection of judicial independence and judicial proceedings;

(q) maintaining registers, whether accessible on a general or restrictive basis, for reasons of general public interest;

(r) safeguarding public health, social security, social protection and humanitarian activity;

(s) safeguarding Cabinet confidentiality;

(s) such other important objectives of general public interest of the Union or the State as may be prescribed in regulations made in accordance with subhead 1 for the purposes of this Head.
3. Regulations made under subhead 1 shall contain specific provisions at least, where relevant, as to:

(a) purposes of the processing or categories of processing;
(b) categories of personal data;
(c) scope of the restrictions introduced;
(d) safeguards to prevent abuse or unlawful access or transfer;
(e) specification of the controller or categories of controllers;
(f) storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
(g) risks to the rights and freedoms of data subjects; and
(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

4. Exercise of the rights provided for in Articles 12 to 22 and Article 34 of the Regulation (as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22), may be restricted by means of regulations made by the Minister for Health, following consultation with the Minister and the Commission, in any case to the extent to which, and for as long as, the application of those provisions would be likely to cause serious harm to the physical or mental health of the data subject.

5. Exercise of the rights provided for in Articles 12 to 22 and Article 34 of the Regulation (as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22) is restricted to the extent that the processing of personal data is necessary for—

(a) the establishment, exercise or defence of legal proceedings and other legal actions or claims, whether in court or in an administrative or out-of-court procedure,

(b) enforcement of civil law claims, including matters relating to any liability of a controller or processor in respect of damages or compensation.

6. Exercise of the rights provided for in Articles 12 to 22 and Article 34 of the Regulation (as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22) is restricted in the case of personal data (including the expression of an opinion
concerning a data subject), where it was given in confidence or on the understanding that it would be treated as confidential.

7. This Head is without prejudice to operation of the Houses of the Oireachtas (Inquiries, Privileges and Procedures) Act 2013.

Explanatory notes
Article 23 of the Regulation permits limited restrictions on controller/processor obligations and the exercise of data subject rights in so far as such restrictions are necessary to safeguard important objectives of general public interests of the Union or a Member State. These restrictions are permitted subject to 3 conditions:

- a legislative measure is required;
- it must be proportionate (“necessary and proportionate measure in a democratic society”)
- the essence of the right to data protection must be respected.

Subhead 2 contains a long – but intentionally non-exhaustive – listing of such general public interests, drawing inspiration from Article 23.1 and recital (73). Subhead 3, based on Article 23.2, specifies the matters (“at least, where relevant”) to be covered in any such legislative measure.

The objective of any regulations made by the Minister or a relevant Minister under this Head would be to protect the processing of personal data in justified cases in order to serve important objectives of general public interest. Section 5 of the Data Protection Act 1988 and section 31 of the UK’s Data Protection Act 1998, have adopted this approach to broadly-similar provisions in the 1995 Data Protection Directive. However, the obligations in the Regulation are set at a higher level and restrictions on the exercise of data subject rights must be justified at a correspondingly higher level.

Subhead 2
Without specifically identifying the controller or processor, subhead 2 lists certain functions – including various investigative, regulatory and adjudicative functions – in respect of which certain restrictions on obligations and the exercise of rights could be justified. These take account of comments and submissions from Government Departments and various public authorities and bodies.

Subhead 4
Subhead 4 reflects Regulations made under section 4(8) of the Data Protection Act 1988 in respect of health professionals (S.I. No. 82 of 1989) and social workers (S.I. No. 83 of 1989). Protection of legal and litigation privilege in respect of both the GDPR and this Act is included in Part 6.

Subhead 6
Subhead 6 incorporates the substance of subsection (4A) of section 4 of the Data Protection Act 1988 (inserted by the 2003 Act. It seeks to protect expressions of opinion given on the basis that the information will be treated in a confidential manner. Its scope will be considered further during the drafting process in order to ensure that it does not provide a means of circumvention relevant data protection standards.

Subhead 7
This Subhead has been included at the request of the Oireachtas Commission.
Head 21: Designation of data protection officer (Article 37)

Provide that:

1. Pursuant to Article 37.4, the Minister may, following consultation with a relevant Minister (if any) and the Commission, make regulations requiring controllers, processors or associations and other bodies representing categories of controllers or processors to designate a data protection officer.

2. Regulations made under this Head may be expressed to apply by reference to one or more of the following—
   (a) a class or classes of controller;
   (b) a class or classes of processor;
   (c) a class or classes of associations or other bodies representing categories of controllers or processors.

3. In making regulations under this Head, the Minister shall have regard to the need for protection of individuals with regard to the processing of their personal data and, without prejudice to the generality of that need, have regard to—
   (a) the nature, scope, context and purposes of the processing,
   (b) risks arising for the rights and freedoms of individuals,
   (c) the likelihood and severity of such risks,
   (d) the costs of implementation.

Explanatory notes
Article 37.1 of the Regulation requires the appointment of a data protection officer in certain cases, including in the case of public authorities and bodies. However, paragraph 4 provides a margin of flexibility for Member States by allowing them to enact national law that would require the appointment of data protection officers in other cases.

This Head seeks to create a regulation-making power so that the flexibility may be availed of in future. It can be expected that the European Data Protection Board will issue guidance in due course, as permitted under Article 70.
Head 22: Limitation on transfers of personal data outside the EU (Article 49.5)

Provide that:

1. Pursuant to Article 49.5, the Minister may, in the absence of an adequacy decision under Article 45 and following consultation with a relevant Minister (if any) and the Commission, make regulations restricting the transfer of specific categories of personal data to a third country or international organisation for important reasons of public interest.

2. Regulations made under this Head may be expressed to apply by reference to one or more of the following—
   (a) a category or categories of personal data,
   (b) a third country or classes of third countries;
   (c) an international organisation.

3. In making regulations under this Head, the Minister shall have regard to the need for protection of individuals with regard to the processing of their personal data and, without prejudice to the generality of that need, have regard to—
   (a) the nature of the personal data,
   (b) the scope, context and purposes of the processing,
   (c) risks arising for the rights and freedoms of individuals,
   (d) the likelihood and severity of such risks for individuals concerned.

Explanatory notes
In the absence of an adequacy decision under Article 45, paragraph 5 of Article 49 gives Member States a margin of flexibility to restrict, for important public interest reasons, the transfer of specific categories of personal data to a third country or an international organisation.

Creation of a regulation-making power allows for the possibility of a speedy response to the existence of such a risk.
Head 23: Imposition of administrative fines on public authorities and bodies (Article 83.7)

Provide that:

1. Pursuant to Article 83.7, an administrative fine may be imposed on a public authority or body in respect of an infringement of the Regulation arising from its activity as an undertaking.

2. In this Head, “undertaking” has the meaning given to it in section 3 of the Competition Act 2002.

Explanatory notes

Article 83 of the General Data Protection Regulation provides for the imposition of substantial fines on data controllers or data processors for infringements of its provisions. However, paragraph 7 provides as follows:

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

A decision not to impose such fines on public authorities and bodies could possibly create competition distortions in areas in which public and private bodies operate in the same space (e.g. public and private hospitals; public and private refuse services).

A possible solution would be to keep the possibility of fines open where public and private bodies provide goods or services in the same market; this would require a distinction to be drawn between categories of public bodies.

A focus on the concept of “undertaking” in competition law is a possible way forward. Irish case law suggests that it is necessary to analyse each activity of a public body separately and consider the circumstances in which it is performed.

The High Court has, for example, ruled that the HSE is an undertaking when providing ambulance services to private patients – Medicall Ambulance Service Ltd v HSE [2011] IEHC 76 – but not when providing the same service to public patients – Lifeline Ambulance Services Ltd v HSE [2012] 432. In Medicall, the Court noted that the HSE was involved in economic activity (as opposed to a regulatory or administrative function) because it provided the service for gain and was in competition with private operators, whereas in Lifeline the Court appeared satisfied that the service for public patients was provided in the public interest and not for gain.
Head 24: Data processing and freedom of expression and information

Provide that:

1. Personal data processed for journalistic purposes and the purposes of academic, artistic or literary expression shall be exempt from a provision of the Regulation specified in subhead 2 if—
   (a) the processing is undertaken for those purposes,
   (b) having regard to the importance of the right to freedom of expression and information in a democratic society, compliance with that provision would be incompatible with such purposes.

2. The provisions referred to in subhead 1 are—
   (a) Chapter II (principles), other than Article 5.1(f),
   (b) Chapter III (rights of the data subject),
   (c) Chapter IV (controller and processor),
   (d) Chapter V (transfer of personal data to third countries and international organisations)
   (e) Chapter VI (independent supervisory authorities),
   (f) Chapter VII (cooperation and consistency).

3. The Commission may, upon its own initiative, refer any question of law arising in a case under subhead 1 to the High Court for determination.

4. An appeal from a determination of the High Court on a question of law under subhead 3 shall lie, by leave of that Court, to the Court of Appeal.

5. In order to take account of the importance of the right to freedom of expression and information in a democratic society, that right shall be interpreted in a broad manner.
Explanatory notes
This Head seeks to give effect to Article 85 of the General Data Protection Regulation which provides that it shall be for Member State law to reconcile the right to protection of personal data with the right to freedom of expression and information.


In the meantime, the Charter of Fundamental Rights has come on stream, Article 11 of which establishes a right to freedom of expression and information. Also relevant is the fact that Article 82 (Right to compensation and liability) of the Regulation clarifies that damages are payable in the case of data breaches giving rise to non-material damage.

The text of subheads 1 and 2 seek to give effect to Article 85. Subhead 3 provides a new ‘case stated’ mechanism which will permit the Commission to refer a question of law arising in relation to the balance to be established between the right to data protection (Article 8 of Charter) and the right to freedom of expression to be referred to the High Court for determination (an appeal to the Court of Appeal will also be possible with permission of the High Court).

Subhead 5 gives expression to the final sentence in recital (153) which states that “in order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.” This is intended to acknowledge activities such as blogging and the expression of views on social media.
Head 25: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Provide that:

1. Subject to subhead 4, Articles 15, 16, 18 and 21 of the Regulation shall not apply to personal data processed for scientific or historical research purposes or statistical purposes in so far as the exercise of the rights set out in these Articles—
   
   (a) is likely to render impossible or seriously impair the achievement of those purposes, and

   (b) the data controller reasonably believes that such derogations are necessary for the fulfilment of those purposes.

2. Subject to subhead 4, Articles 15, 16, 18, 19, 20 and 21 shall not apply to personal data processed for archiving purposes in the public interest in so far as the exercise of the rights set out in these Articles—

   (a) is likely to render impossible or seriously impair the achievement of those purposes, and

   (b) the controller reasonably believes that such derogations are necessary for the fulfilment of those purposes.

3. Where data processing referred to in subheads 1 and 2 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those subheads.

4. Processing for the purposes referred to in subheads 1 and 2 shall be subject to appropriate safeguards for the rights and freedoms of the data subject, including technical and organisational measures to ensure respect for the principle of data minimisation; where such purposes can be fulfilled by processing which does not permit, or no longer permits, identification of data subjects, the purposes shall be fulfilled in that manner.

Explanatory notes

This Head seeks to give effect to Article 89 of the Regulation which provides for derogations, subject to certain conditions, from specified data subject rights in Chapter III of the Regulation for
‘privileged purposes’ (i.e. processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes). Recital (156) provides as follows:

The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

Recitals (157) to (163) are also relevant to this Head.

Article 89 does not include a provision on the limitation on the right to erasure (right to be forgotten) as such a limitation is provided for in Article 17.3(d) of the Regulation.
Part 4 - Implementation of Data Protection Directive

Chapter 1
General Provisions

Head 26 – Interpretation

Provide that:
1. In this Part, unless the context otherwise requires—

“biometric data” means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual [such as facial images or dactyloscopic data];

“competent authority” means:

(a) a public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or

(b) any other entity authorized by national law to exercise public authority and public powers for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

“data concerning health” means data related to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status;

“controller” means the competent authority which alone or jointly with others determines the purposes and means of the processing of personal data except where the data controller, or the specific criteria for designation of the data controller, is specified in Union or national law;
“processor” means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of a data controller but does not include an employee who processes such data in the course of his or her employment;

“national law” includes a statute and an instrument made under a power conferred by a statute;

“genetic data” means all personal data, relating to genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question;

“international organisation” means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries;

“national security” includes—

(a) protecting the security of the State, including, but not limited to, the following:
   (i) preventing, detecting and investigating offences under the Offences against the State Acts 1939 to 1998, the Criminal Law Act 1976, the Criminal Justice (Terrorist Offences) Act 2005 and the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010;
   (ii) protecting the State from—
      (I) espionage,
      (II) sabotage,
      (III) unlawful acts that subvert or undermine, or are intended to subvert or undermine, parliamentary democracy or the institutions of the State, and
      (IV) acts of foreign interference that are, or are intended to be, detrimental to the interests of the State and are clandestine or deceptive or involve a threat to any person, whether directed from, or committed or intended to be committed within, the State or not,

(b) identifying foreign capabilities, intentions or activities within or relating to the State that impact on the international well-being or economic well-being of the State, and
(c) co-operating with authorities in other states and international organisations aimed at preserving international peace, public order and security;

“personal data” means any information relating to an identified or identifiable living individual (“data subject”); an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual;

“personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

“processing” means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“profiling” means any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

“pseudonymisation” means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately by the controller and is subject to technical and organizational measures to ensure its non-attribution to an identified or identifiable individual;

“recipient” means a natural or legal person, public authority, agency or any other body, to which the personal data are disclosed, whether a third party or not; public authorities and bodies which may receive data in the framework of a particular inquiry in accordance with national law shall not
be regarded as recipients; the processing of these data by those public authorities and bodies shall be in compliance with the applicable data protection rules according to the purposes of the processing;

“relevant filing system” means any set of structured personal data, either by reference to individuals or by reference to criteria relating to individuals, which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

“restriction of processing” means the marking of personal data under the control of the controller for the purpose of limiting their processing in the future;

“special categories of personal data” means—

(a) data revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership of a data subject,

(b) genetic data and biometric data processed for the purpose of uniquely identifying an individual,

(c) data concerning a data subject’s health or sexual life or sexual orientation;

“third country” means a State other than a Member State.

2. A word or expression that is used in this Part and also in the Directive has, unless the context otherwise requires, the same meaning in this Part as it has in the Directive.

3. For the purpose of determining appropriate technical and organizational measures to be taken by the controller or processor in order to ensure compliance with the requirements of this Part, the controller and processor shall, where relevant, have due regard for the following—

a. nature of the personal data concerned,

b. level of access to such personal data,
c. nature, scope, context and purposes of the processing,
d. severity of risks for the rights and freedoms of individuals arising from such processing,
e. the state of the art and cost of implementation,
f. guidelines, recommendations and best practices issued by the Commission or the European Data Protection Board.

**Explanatory notes**

Most of the definitions have been taken from Article 3 of the Directive.

As regards the scope of the definition of “competent authority”, recital (11) states, inter alia, “... a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive.” (Emphasis added)

In the Irish legal system, many public authorities and bodies have law enforcement functions and will be covered by this Part when discharging those, but only those, functions. Otherwise, the GDPR will apply.

The definition of ‘national security’ is based on the definition in the Garda Síochána Act 2005, as amended. Subhead 3 is intended to assist controllers and processors in determining the measures to be taken for the purposes of ensuring compliance with this Part. The factors included are drawn from Articles 19 (Obligations of the controller), 20 (Data protection by design and default) and 29 (Security of processing).
Head 27 – Application of this Part

Provide that:

1. This Part applies to the processing of personal data by a competent authority for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security [Articles 1.1 and 2.1].

2. This Part applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a relevant filing system or are intended to form part of such a system [Article 2.2].

3. Where a competent authority performs tasks other than those performed for purposes referred to in subhead 1, Regulation (EU) 2016/679 shall apply to processing related to such other tasks [Article 9.2].

4. Personal data processed for purposes referred to in subhead 1 shall not be processed for purposes other than those purposes unless such processing is authorised by Union or national law; Regulation (EU) 2016/679 shall apply to such processing [Article 9.1 of Directive].

5. This Part shall not apply to processing in the course of an activity which falls outside the scope of Union law [Article 2.3].

Explanatory Notes

Subhead 1 gives effect to the content of Articles 1.1 and 2.1; subhead 2 gives effect to Article 2.2.

Recital (12) states:

*The activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law enforcement authorities where necessary to safeguard against and prevent threats to public security and*
to fundamental interests of the society protected by law which may lead to a criminal offence. Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of Regulation (EU) 2016/679.

Recital (18) reads, inter alia, as follows:

The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Directive.

Subhead 3 gives effect to Article 9.2. It means, for example, that personal data processing by Gardaí in relation to passport applications will be governed by the GDPR rather than this Part which gives effect to the Directive.

Subhead 4 gives effect to Article 9.1. It means, for example, that where personal data are to be transferred to the National Archives for archiving purposes, the Regulation’s provisions will apply. Also, if such data are used for scientific purposes unrelated to the scope of subhead 1, the Regulation applies. Scientific research within the scope of subhead 1 (e.g. concerning recidivism) would fall under this legislation.

As regards subhead (5), Article 2.3(a) states that the Directive does not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law. Recital (14) reads as follows:

Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) should not be considered to be activities falling within the scope of this Directive.
Head 28 – Collection, processing, keeping and use of personal data

Provide that:

1. Personal data shall be [Article 4]:
   (a) processed lawfully and fairly;
   (b) collected for one or more specified, explicit and legitimate purposes and not processed in a manner that is incompatible with such purposes;
   (c) adequate, relevant and not excessive in relation to the purposes for which they are processed;
   (d) accurate and, where necessary, kept up to date; every reasonable step shall be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
   (f) processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

2. Processing of personal data shall be lawful to the extent that such processing is necessary for the performance of a function by a competent authority for purposes set out in Head 27.1. [Article 8].

3. Processing by the same or another competent authority for any of the purposes referred to in Head 27.1 other than that for which the data have been collected is permitted in so far as the processing is necessary and proportionate for the performance of that function [Article 4.2].

4. Purposes referred to in Head 27.1 include archiving in the public interest, scientific, statistical or historic use by the same or another controller, subject to appropriate safeguards for the rights and freedoms of data subjects [Article 4.3].

5. Competent authorities shall determine, in a transparent manner, appropriate time limits for erasure of personal data within their control or for periodic reviews of the need for retention of
such data, and shall ensure by means of procedural measures that such time limits or periodic reviews are observed. [Article 5].

6. Competent authorities shall be responsible for and be able to demonstrate compliance with this Head [Article 4.4].

7. A processor and any person acting under the authority of the competent authority or processor who has access to personal data shall not process the data except on instructions from the competent authority unless required to do so by Union or national law [Article 23].

**Explanatory Notes**

This Head broadly corresponds to section 2 of the 1988 Act, as amended.

Subhead 1 gives effect to the data protection principles in Article 4.1 of the Directive. Recital (26) reads as follows:

*Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not in itself prevent the law enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned. The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms ('ECHR'). Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular, the specific purposes for which the personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Member States should lay down appropriate safeguards for personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use.*

Recital (30) reads:
The principle of accuracy of data should be applied while taking account of the nature and purpose of the processing concerned. In particular, in judicial proceedings, statements containing personal data are based on the subjective perception of natural persons and are not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

Subhead 2 defines what is mean by ‘lawful’ processing and gives effect to Article 8.1. Subhead 3 gives effect to Article 4.2, while subhead 4 transposes Article 4.3. Subhead 5 seeks to give effect to the new provision in Article 5. The accountability principle is encompassed in subhead 6.
Head 29 – Security measures for personal data

Provide that:

1. When determining appropriate technical or organisational measures for the purposes of Head 28 (1)(f) and Head 47, competent authorities and processors shall ensure that such measures provide a level of security appropriate to the harm that might result from accidental or unlawful destruction, loss, alteration of, or unauthorised disclosure of or access to the personal data concerned.

2. Competent authorities and processors shall take all reasonable steps to ensure that persons employed by them and other persons at the place of work are aware of and comply with relevant measures.

Explanatory notes
This Head gives further effect to subhead 1(f) of Head 28. Section 2C of the 1988 Act (as inserted by section 4 of the 2003 Act) contains broadly similar provisions.
Head 30 – Data quality

Provide that:

1. Where relevant, competent authorities shall as far as possible distinguish between the personal data of different categories of data subjects [Article 6].

2. Competent authorities shall as far as possible ensure that personal data based on facts are distinguished from personal data based on personal assessments [Article 7.1].

3. Competent authorities shall [Article 7.2]—
   (a) take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up-to-date are not transmitted or otherwise made available,
   (b) as far as practicable, verify the quality of personal data before they are transmitted or made available,
   (c) as far as possible, in transmissions of personal data, provide any necessary information to enable a recipient to assess the degree of accuracy, completeness and reliability of those data, and the extent to which they are up-to-date.

4. Where incorrect personal data have been transmitted, or such data have been unlawfully transmitted, the competent authority shall notify the recipient without delay; in such cases, the personal data shall be rectified, erased or restricted as the case may be [Article 7.3].

Explanatory Notes
This Head is intended to give effect to Article 6 (subhead 1) and Article 7 (subheads 2 to 4) of the Directive, neither of which form part of existing data protection law. The text of the former contains the following examples:
   (a) persons with regard to whom there are serious grounds for believing that they have committed, or are about to commit, a criminal offence;
   (b) persons convicted of a criminal offence;
   (c) victims of a criminal offence, or those with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence; and
(d) third parties to the criminal offence, such as those who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or those who can provide information on criminal offences, or a contact or associate of an individual referred to at (a) and (b).

The inspiration for Article 6 appears to derive from a Council of Europe recommendation. Nonetheless, recital (31) reads *inter alia* as follows:

..... *This should not prevent the application of the right of presumption of innocence as guaranteed by the Charter and by the ECHR, as interpreted in the case law of the Court of Justice and by the European Court of Human Rights respectively.*
Head 31 - Processing of special categories of personal data

Provide that:

1. Special categories of personal data may be processed only where—
   (a) authorised by Union or national law,
   (b) the processing is necessary in order to protect the vital interests of the data subject or another individual, or
   (c) the personal data have been or are made public by the data subject.

2. A data subject may agree to the processing of his or her personal data for the purposes of this Part such as, for example, DNA tests in criminal investigations or the monitoring of his or her location with electronic tags in connection with criminal proceedings or the execution of criminal penalties.

3. The processing of special categories of personal data shall be subject to appropriate safeguards for the rights and freedoms of the data subject.

Explanatory notes
This Head seeks to give effect to Article 10 of the Directive. Processing of special categories of personal data is currently permitted under section 2B, inserted by the Data Protection (Amendment) Act 2003, of the Data Protection Act 1988. Recital (37) reads inter alia:

.... Appropriate safeguards for the rights and freedoms of the data subject could include the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data. The processing of such data should also be allowed by law where the data subject has explicitly agreed to the processing that is particularly intrusive to him or her. However, the consent of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities.

While data subject consent is not as a rule accepted as a lawful basis for processing, recital (35) allows data subject agreement in certain cases; this is reflected in subhead 2.
Chapter 2
Data subject rights

Head 32 – Restriction on automated individual decision making

Provide that:

1. A decision which produces an adverse legal effect for a data subject, or otherwise significantly affects him or her, shall not be based solely on automated processing of personal data (including profiling) except where authorised by Union or national law containing appropriate safeguards, including the right to obtain human intervention on the part of the competent authority.

2. Subhead 1 shall not apply if a decision—
   (a) is authorised or required by national law and the data subject has been informed of the proposal to make the decision, and
   (b) adequate steps have been taken to safeguard the legitimate interests of the data subject by, for example (but without prejudice to the generality of the foregoing), the making of arrangements to enable him or her to make representations in relation to the decision.

3.(a) A decision referred to in paragraph 1 shall not be based on special categories of personal data unless suitable measures to safeguard the data subject’s rights, freedoms and legitimate interests are in place.

(b) Profiling that results in discrimination against individuals on the basis of special categories of personal data is prohibited in accordance with Union law.

Explanatory notes
This Head seeks to give effect to Article 11 of the Directive. Section 6B of the 1988 Act (as inserted by section 8 of the 2003 Act) constrains broadly similar provisions.
Head 33 – Right to information (Article 13)

Provide that:

1. Subject to Head 37, a competent authority shall ensure that a data subject is provided with, or has made available to him or her, the information specified in subhead (2)—

   (a) within a reasonable period after obtaining the personal data (but at the latest within one month) having regard to the specific circumstances in which the personal data are processed;

   (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject.

2. The information referred to in subhead 1 is the following—

   (a) identity and contact details of the competent authority, and contact details of its data protection officer;

   (b) purpose or purposes for which the personal data are intended to be processed,

   (c) existence of the right to request access to and rectification, erasure or restriction of processing of the personal data;

   (d) right to lodge a complaint with the Commission and the Commission’s contact details;

   (e) in specific cases, such further information which, having regard to the circumstances in which the personal data are or have been collected, or are to be processed, is necessary to enable the data subject to exercise his or her rights, including—

      (i) the legal basis for the processing,

      (ii) the period during which the personal data will be retained (or if not possible, the criteria used to determine such period),

      (iii) where applicable, categories of recipients of the personal data.

3. The information referred to in paragraphs (a) to (d) of subhead 2 may be made available to a data subject in clear and plain language on the competent authority’s web site.
4. Without prejudice to Head 37, subhead 2 does not apply insofar as—

(a) the data subject already has the information, or

(b) provision of such information proves impossible or would involve a disproportionate effort, in particular in the case of archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

**Explanatory notes**

This Head seeks to give effect to Article 13 (Information to be given to the data subject). The time limits in subhead 1 come from Article 14.3 of the GDPR.

Subheads 2 and 3 are derived from recital (42) which reads as follows:

> At least the following information should be made available to the data subject: the identity of the controller, the existence of the processing operation, the purposes of the processing, the right to lodge a complaint and the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing. This could take place on the website of the competent authority. In addition, in specific cases and in order to enable the exercise of his or her rights, the data subject should be informed of the legal basis for the processing and of how long the data will be stored, in so far as such further information is necessary, taking into account the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject. [Emphasis added]

The restrictions in subhead 4 are based instead on corresponding provisions in Articles 13 and 14 of the GDPR.

This Head provides for an extended right to information compared with section 2D of the 1988 Act (as inserted by section 4 of the 2003 Act).
Head 34 – Right of access (Article 14)

Provide that:

1. Subject to Head 37, a data subject who considers that personal data concerning him or her have been or are being processed by or on behalf of a competent authority shall, if he or she so requests the authority in writing, have the right to—

   (a) be informed whether any such data have been or are being processed, and

   (b) if such data have been or are being processed, be provided with the following information—

   (i) the purpose and legal basis for the processing,
   (ii) the categories of personal data concerned,
   (iii) the recipients or categories of recipients to whom the personal data have been disclosed,
   (iv) where possible, the retention period or, if not possible, the criteria used for determining the retention period,
   (v) the existence of the right to request rectification or erasure of his or her personal data or restriction of processing of the data,
   (vi) the right to lodge a complaint with the Commission and the Commission’s contact details,
   (vii) communication of the personal data being processed and any available information concerning their origin,

as soon as may be and in any event not more than one month after the request has been made.

2. Information provided under subhead 1 shall not reveal, or be capable of revealing, the identity of an individual who supplied information in confidence or on condition that it would be treated as confidential; in such cases it shall be sufficient that the data subject be provided with a summary of the personal data concerned in an intelligible form which permits exercise of his or her rights under this Part.

Explanatory notes

Subhead 1 seeks to give effect to Article 14 (Right of access by the data subject). Sections 3 and 4 of the 1988 Act already provide for extensive rights to establish the existence of and access to personal data. Subhead 2 is based on content in recital (43).
Head 35 – Right to rectification, erasure or restriction of processing

Provide that:

1. Subject to Head 37, a data subject, if he or she so requests a competent authority processing his or her personal data, shall have the right—
   (a) to have inaccurate or incomplete personal data rectified or completed, as the case may be,
   (b) to have personal data erased in compliance with a legal obligation to which the controller is subject.

2. The competent authority shall comply with the request as soon as may be and in any event not more than one month after it has been made.

3. Instead of erasure, the competent authority shall restrict processing where—
   (a) the accuracy or completeness of personal data is contested by a data subject and their accuracy or completeness cannot be ascertained, or
   (b) the personal data are required for evidential purposes.

4. Where processing has been restricted under subhead 3, the competent authority shall inform the data subject prior to lifting the restriction.

5. Where a competent authority complies, or is deemed to have complied, with a request under subheads 1, 2 or 3, it shall, as soon as may be and in any event not more than one month after the request has been given or sent to him or her, notify—
   (a) the data subject concerned,
   (b) any competent authority from which the inaccurate or incomplete personal data have been received, and
   (c) any recipient of the inaccurate or incomplete personal data for the purposes of rectification, erasure or restriction by them,

of the rectification, erasure or restriction concerned.

6. The right to rectification under this Head shall not apply to the content of witness statements.
7. For the purposes of this Head, data are inaccurate if they are incorrect or misleading as to any matter of fact.

**Explanatory notes**

This Head gives effect to Article 16 of the Directive (Right to rectification, erasure and restriction of processing). Subhead 6 picks up a restriction on the right to rectification mentioned in recital (47).

Section 6 of the 1988 Act (as amended by section 7(b) of the 2003 Act) provides a right to rectification or erasure of personal data. Subhead 7 reproduces section 1(2) of the 1988 Act.
Head 36 – Communication with data subjects (Article 12)

Provide that:

1. Competent authorities shall facilitate the exercise of data subject rights and shall take all reasonable steps to provide information under Head 33 and any communication under Heads 34 and 35 to data subjects in a concise, intelligible and easily accessible form, using clear and plain language.

2. The information referred to in paragraph 1 shall be provided by appropriate means, including by electronic means; as a general rule, competent authorities shall provide the information in the same form as the request.

3. Competent authorities shall inform data subjects about the follow-up given to specific requests under Heads 33, 34 and 35 without undue delay.

4. Information provided to data subjects under Head 33 and any communications and actions by competent authorities under Heads 34 and 35 shall be free of charge.

5. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, a competent authority may charge a reasonable fee taking into account the administrative costs of compliance with the request, or may refuse to act on the request; in the latter case, the competent authority shall demonstrate the manifestly unfounded or excessive character of the request.

6. Where a competent authority has reasonable doubts concerning the identity of an individual making a request under Heads 34 and 35, submission of such additional information as required in order to confirm the identity of the data subject may be requested.

Explanatory notes

This Head gives effect to Article 12 of the Directive.
Head 37 – Restrictions

Provide that:

1. With due regard for the fundamental rights and legitimate interests of the data subject—
   
   (a) compliance with the requirement for a competent authority to make available to the data subject the information referred to in Head 33(2)(e) [Article 13.3],

   (b) compliance with a request of the data subject to be informed whether his or her personal data have been or are being processed and, if so, to have access to the data under Head 34 [Article 15],

   (c) compliance with the requirement for a competent authority to inform the data subject of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal under Head 35 [Article 16.4],

may be delayed or restricted, wholly or partly, to the extent that and for as long as such a restriction constitutes a necessary and proportionate measure in a democratic society, where the competent authority considers that such provision could reasonably be expected to—

(i) endanger the life, safety or well-being of an individual,
(ii) facilitate the commission of an offence,
(iii) prejudice or impair national security, defence of the State, or its international relations,
(iv) obstruct or impair official or legal inquiries, investigations or procedures or the operation of legal privilege,
(v) prejudice or impair—
   (I) the prevention, detection or investigation of offences, the apprehension or prosecution of offenders or the effectiveness of lawful methods, systems, plans or procedures employed for the purposes of the matters aforesaid,
   (II) the enforcement of, compliance with or administration of any enactment,
   (III) the safety of the public and the safety or security of individuals and property,
   (IV) the fairness of criminal proceedings in a court or other tribunal,
   (V) the security of—
      a. a penal institution,
      b. a children detention school within the meaning of section 3 of the Children Act 2001,
      c. a remand centre designated under section 88 of the Children Act 2001,
      d. the Central Mental Hospital,
      e. any system of communications, whether internal or external, of the Garda Síochána, the Defence Forces, the Revenue Commissioners or a penal institution.
2. The Minister, following consultation with the Commission, or a relevant Minister, following consultations with the Minister and the Commission, may by regulations specify categories of processing which wholly or partly fall under (i) to (v) of subhead 1.

3. Subject to subhead 4, where (b) or (c) of subhead 1 applies the competent authority shall inform the data subject in writing, as soon as may be and in any event not more than one month after the request has been made, of any refusal or restriction of access and the reasons for such refusal or restriction and the right to lodge a complaint with the Commission or to seek a judicial remedy.

4. Subhead 3 shall not apply where the provision of the information would undermine a purpose under subhead 1; in such cases, the competent authority shall inform the data subject of possible recourse to the Commission under Head 38 or a judicial remedy.

5. Where a competent authority refuses, wholly or partially, a data subject’s request under (b) or a requirement on the competent authority under (c) of subhead 1, it shall document the factual or legal reasons on which the decision is based and shall make that information available to the Commission if requested by the Commission so to do.

6. Subject to Chapter 4 of the Criminal Justice (Forensic Evidence and Database System) Act 2014 (as amended by this Act), this Chapter shall not apply to the Forensic Science Laboratory of the Department of Justice and Equality, insofar as it relates to records concerning, or arising from, the forensic criminal investigation functions performed by that Laboratory, including the analysis of specimens or in connection with an investigation being undertaken by An Garda Síochána or the Garda Síochána Ombudsman Commission and the approval, supply, testing and maintenance of apparatus and of equipment.

**Explanatory notes**

This Head seeks to give effect to Articles 13.3, 15 and 16.4 which allow for restrictions of data subject rights to information, access and rectification or erasure respectively. Recital (43) reads:

*A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know, and obtain communications about, the purposes for which the data are*
processed, the period during which the data are processed and the recipients of the data, including those in third countries. Where such communications include information as to the origin of the personal data, the information should not reveal the identity of natural persons, in particular confidential sources. For that right to be complied with, it is sufficient that the data subject be in possession of a full summary of those data in an intelligible form, that is to say a form which allows that data subject to become aware of those data and to verify that they are accurate and processed in accordance with this Directive, so that it is possible for him or her to exercise the rights conferred on him or her by this Directive. Such a summary could be provided in the form of a copy of the personal data undergoing processing.

Recital (44) reads inter alia

.... The controller should assess, by way of a concrete and individual examination of each case, whether the right of access should be partially or completely restricted.

Subhead 4 is intended to enable controllers to ‘neither confirm nor deny’ the existence of personal data. Section 33(4) of the Freedom of Information Act 2014 contains the following provision which has a similar purpose:

Where an FOI request relates to a record to which subsection (1) applies, or would, if the record existed, apply, and the head concerned is satisfied that the disclosure of the existence or non-existence of the record would prejudice a matter referred to in that subsection, he or she shall refuse to grant the request and shall not disclose to the requester concerned whether or not the record exists.

Subhead 5 makes provision for oversight by the Data Protection Commission. Section 5 of the Data Protection Act 1988 already allows for restrictions on the right of access.

Subhead 6 contains a derogation from this Chapter for the Forensic Science Laboratory since Chapter 4 of the Criminal Justice (Forensic Evidence and Database System) Act 2014 (as amended by this legislation) makes specific provision for the exercise of data subject rights.
Head 38 – Indirect exercise of rights and verification by Commission

Provide that:

1. Where a restriction under Head 37 applies, the data subject may seek verification or review by the Commission.

2. In such cases, the Commission shall inform the data subject at least that all necessary verifications or a review by it has taken place; the Commission shall also inform the data subject of his or her right to seek a judicial remedy.

Explanatory notes

This Head seeks to give effect to indirect exercise of data subject rights under Article 17 of the Directive.
Head 39 – Exercise of rights in criminal proceedings

Provide that:

Where personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings, exercise of the rights referred to in Heads 33, 34 and 35 shall be in accordance with rules of court.

Explanatory notes

Recital (49) reads:

Where the personal data are processed in the course of a criminal investigation and court proceedings in criminal matters, Member States should be able to provide that the exercise the right to information, access to and rectification or erasure of personal data and restriction of processing is carried out in accordance with national rules on judicial proceedings.
Chapter 3
Data controller and data processor obligations

Head 40 – Obligations of competent authority

Provide that:

1. Competent authorities shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is compliant with this Part; such measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in subhead 1 shall include the implementation of appropriate data protection policies by the competent authority.

3. Where two or more competent authorities jointly determine the purposes and means of the processing, they are joint controllers and shall determine their respective compliance responsibilities in a transparent manner by means of an arrangement between them (except and in so far as their respective responsibilities are determined by Union or national law).

4. The arrangement referred to in subhead 3 shall designate the point of contact for data subjects unless this is determined by national law; irrespective of the terms of this arrangement, a data subject may exercise his or her rights in respect of and against any of the competent authorities.

Explanatory notes

Subheads 1 and 2 of this Head seek to give effect to Article 19 of the Directive. Subheads 3 and 4 do likewise in respect of Article 21
Head 41 – Data protection by design and by default

Provide that:

1. A competent authority shall, both at the time of the determination of the means of processing and at the time of processing, implement appropriate technical and organisational measures which are designed to protect the rights and freedoms of data subjects.

2. A competent authority shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose are processed; this applies to the amount of data collected, the extent of the processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of persons.

Explanatory notes
This Head seeks to give effect to Article 20 of the Directive.
Head 42 – Processor

Provide that:

1. Where processing is to be undertaken by a processor, competent authorities shall engage only processors providing sufficient guarantees that processing will meet the requirements of this Part and ensure the protection of the rights and freedoms of data subjects; such processing shall be carried out under a contract in writing between the competent authority and processor concerned or in accordance with Union or national law [Article 22.1].

2. In addition to the matters referred to in Head 29, the contract referred to in subhead 1 shall specify the subject matter, duration, nature and purpose of the processing, the types of personal data and categories of data subjects, the obligations and rights of the competent authority and shall stipulate in particular that the processor shall [Article 22.2 and 3]:
   (a) act only on instructions from the competent authority unless required to do so by Union or national law;
   (b) not procure the services of another processor without the prior authorisation of the competent authority in writing;
   (c) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
   (d) assist the competent authority to ensure compliance with this Part’s provisions on the exercise of data subject rights;
   (e) erase or return the personal data following completion of the processing and delete existing copies unless Union or national law requires retention of the data;
   (f) make available to the competent authority all information necessary to demonstrate compliance with the obligations laid down in this Head.

3. The processor and any person acting under the authority of the competent authority or processor who has access to personal data shall not process the data except on instructions from the competent authority unless required to do so by Union or national law.
4. A processor shall inform the competent authority of any intended changes concerning the addition or replacement of other processors thereby giving the competent authority the opportunity to object to such changes.

5. Where a processor determines the purposes and means of processing, that processor shall be a controller in respect of that processing for the purposes of this Part.

**Explanatory notes**

This Head seeks to give effect to Article 22 (Processor) and 23 (Processing under the authority of the controller and processor) which, inter alia, require a formal contract or other legal act governing relations between the data controller and the data processor.
Head 43 – Records of data processing activities

Provide that:

1. A competent authority shall maintain a record of categories of data processing activities under its responsibility containing the following information:

   (a) name and contact details of the competent authority, any joint controller and the data protection officer;
   (b) purposes of the data processing;
   (c) categories of recipients to whom the personal data have been or will be disclosed;
   (d) description of categories of data subjects and of the categories of personal data;
   (e) where applicable, the use of profiling;
   (f) where applicable, the categories of transfers of personal data to a third country or an international organisation;
   (g) an indication of the legal basis of the processing activity, including transfers, for which the data are intended;
   (h) where possible, the envisaged time limits for erasure of the different categories of personal data;
   (i) where possible, a general description of the relevant technical and organisational measures.

2. A processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

   (a) name and contact details of the processor or processors, each competent authority on behalf of which the processor is acting and the data protection officer (if any);
   (b) categories of data processing carried out on behalf of each competent authority;
   (c) where applicable, transfers of personal data to a third country or an international organisation where explicitly instructed to do so by the competent authority, including the identification of that third country or international organisation;
   (d) where possible, a general description of the technical and organisational security measures referred to in [Head 47/Article 29(1)].

3. The records referred to in subheads 1 and 2 shall be in writing; on request, competent authorities and processors shall make such records available to the Commission for inspection and examination.

Explanatory notes

This Head seeks to give effect to Article 24 of the Directive. The definition of “writing” in the Interpretation Act 2005 includes information in non-legible form that may be stored electronically.
Head 44 – Data logging obligations

Provide that:

1. Data logs shall be maintained of at least the following interventions in automated processing systems: collection, alteration, consultation, disclosure (including transfer), combination or erasure.

2. The data logs referred to in subhead 1 shall make it possible to establish the—
   (a) date and time of an intervention,
   (b) reason or reasons for the intervention,
   (c) identity of the individual who made the intervention, and
   (d) identity of any recipients of such personal data.

3. Data logs shall be used solely for the purposes of verifying the lawfulness of the processing, self-monitoring, ensuring data integrity and security, and criminal proceedings.

4. The competent authority or processor shall, on request, make data logs available to the Commission for inspection and examination.

5. Subject to subhead 6, automated processing systems established before 6 May 2016 shall be complaint with this Head by 6 May 2023 [Article 63.2].

6. Where it would otherwise cause serious difficulties for the operation of an automated processing system, the period referred to in subhead 5 may be extended but not beyond 6 May 2026 [Article 63.3].

Explanatory notes
Subheads 1 to 4 seek to give effect to Article 25 of the Directive. Recital (57) reads:

Logs should be kept at least for operations in automated processing systems such as collection, alteration, consultation, disclosure including transfers, combination or erasure. The identification of the person who consulted or disclosed personal data should be logged and from that identification it should be possible to establish the justification for the processing operations. The logs should solely be used for the verification of the lawfulness of the processing, self-monitoring, for ensuring data integrity and data security and criminal proceedings. Self-monitoring also includes internal disciplinary proceedings of competent authorities.
Article 25 is based on article 10 of the Council Framework Decision 200/977/JHA on the protection of personal data in the framework of police and judicial cooperation in criminal matters. The effect of this head is to extend logging requirements to all competent bodies.

Article 63 of the Directive allows for an extended period for the implementation of this requirement in respect of automated processing systems set up before 6 May 2016 where implementation involves disproportionate effort.
Head 45 – Cooperation with the Commission

Provide that:

Competent authorities and processors shall, on request by the Commission, co-operate with and assist the Commission in the performance of its tasks and exercise of its powers under this Part.

Explanatory notes

This obligation is required under Article 26 of the Directive.
Head 46 – Data protection impact assessment and prior consultation with Commission

Provide that:

1. Where, having regard to its nature, scope, context and purposes, a type of data processing is likely to result in a high risk for the rights and freedoms of individuals, the competent authority shall carry out an assessment of its likely impact on the protection of personal data prior to the commencement of processing.

2. The impact assessment referred to in subhead 1 shall contain at least the following—

   (a) a general description of the intended processing,

   (b) an assessment of the risks arising from such processing for the rights and freedoms of data subjects, and

   (c) a description of intended safeguards, security measures and mechanisms to mitigate risks and ensure the protection of personal data in compliance with the provisions of this Part.

3. The competent authority shall consult the Commission prior to the commencement of processing where an impact assessment indicates that despite mitigation measures the processing would result in high risk for the rights and freedoms of data subjects.

4. For the purpose of subhead 3, the competent authority shall provide the Commission with the impact assessment and, on request, with any other information required by the Commission to enable it to assess the risks for the rights and freedoms of data subjects and compliance of intended processing with the provisions of this Part.

5. Where, following consultation, the Commission considers that intended processing would not comply with the provisions of this Part, in particular where the competent authority has insufficiently identified or mitigated risks for the rights and freedoms of data subjects, the Commission shall, within six weeks of receiving the consultation request, give written advice to the competent authority and, where applicable the processor, and may use any of the powers referred to in Head 61.
6. The period referred to in subhead 5 may be extended for a further four weeks having regard to the complexity of the intended processing; in such cases, the competent authority and, where applicable, the processor shall be informed of the delay within a month of receiving the consultation request and the reasons for it.

7. Notwithstanding subhead 3, the Commission may establish a list of processing activities which shall be subject to the prior consultation obligation referred to in that subhead; subheads 4, 5 and 6 shall apply as appropriate.

8. For the purposes of this Part, the Commission shall be consulted during the preparation of proposals for legislation and statutory instruments that relate to processing of personal data (Article 28.2).

**Explanatory notes**

This Head seeks to give effect to Article 28 of the Directive. Recital 58 reads inter alia:

> .... Impact assessments should cover relevant systems and processes of processing operations, but not individual cases.
Head 47 – Security of processing

Provide that:

1. Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of processing as well as risks of varying likelihood and severity for the rights and freedoms of individuals, competent authorities and processors shall implement appropriate technical and organisational measures in order to ensure an appropriate level of security.

2. In the case of automated data processing, competent authorities and processors shall, following an evaluation of the risks referred to in subhead 1, implement measures designed to:

   (a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);
   (b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
   (c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);
   (d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);
   (e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);
   (f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);
   (g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input (input control);
   (h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);
   (i) ensure that installed systems may, in case of interruption, be restored (recovery);
   (j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored personal data cannot be corrupted by means of a malfunctioning of the system (integrity).

Explanatory notes

This Head gives effect to the security obligations in Article 29 of the Directive.
Head 48 – Notification of personal data breach to Commission

Provide that:

1. In the event of a personal data breach, the competent authority shall, without undue delay and, where feasible, no later than 72 hours of becoming aware of it, notify the Commission of the breach; where it has not been notified within the 72-hour period, the notification shall be accompanied by an explanation by the competent authority of the reasons for the delay.

2. Subhead 1 shall not apply where, taking account of the nature of the personal data and the scope, context and purposes of processing, the personal data breach is unlikely to result in a risk for the rights and freedoms of data subjects.

3. The notification referred to in subhead 1 shall contain—
   (a) a description of the personal data breach including, where possible, the categories and number of data subjects concerned, and details of personal data records concerned;
   (b) descriptions of—
      (i) the likely consequences of the personal data breach, and
      (ii) measures taken or proposed to be taken to mitigate any possible adverse effects;
   (c) the name and contact details of the data protection officer, or other point of contact at which more detailed information can be obtained.

4. Where it is not possible to provide all the information required in the notification at the same time, it may be provided, without undue delay, on a phased basis.

5. Competent authorities shall retain a detailed record of the personal data breach, its effects and the measures taken to mitigate any possible adverse effects, and provide this record to the Commission if requested to do so.

6. Where a data breach involves personal data that have been transmitted by or to a controller in another Member State, the information referred to in subhead 3 shall be communicated by the competent authority to that controller without undue delay.
7. Processors shall notify the relevant competent authority without undue delay after becoming aware of a personal data breach.

Explanatory notes
This Head gives effect to the notification obligation in Article 30 of the Directive.

The non-statutory, Personal Data Security Breach Code of Practice, which was adopted by the Data Protection Commissioner under section 13(2)(b) of the 1988 Act (as substituted by section 14(1)(a) of the 2003 Act) already sets out rules in relation to the notification of data breaches to the Commissioner and to data subjects.
Head 49 – Communication of personal data breach to data subject

Provide that:

1. Where a personal data breach is likely to result in high risk for the rights and freedoms of data subjects, the competent authority shall communicate details of the breach to the data subjects concerned without undue delay.

2. The communication referred to in subhead 1 shall not be required if any of the following conditions are met:
   (a) the competent authority had implemented appropriate protection measures, in particular those that render personal data unintelligible to those not authorised to access the data, such as encryption;
   (b) the competent authority has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in subhead 1 is no longer likely to materialise;
   (c) it would involve a disproportionate effort; in such a case, the competent authority shall publish, or have published, a communication whereby all data subjects concerned are informed in an equally effective manner.

3. The communication to the data subject referred to in subhead 1 shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information provided for in paragraphs (b) and (c) of Head 48.3.

4. Where a competent authority has not communicated a personal data breach to data subjects concerned, the Commission may, on receipt of the notification referred to in Head 48 and having considered the likelihood of the breach resulting in high risk for data subjects, require the competent authority to do so, or may decide that any of the conditions referred to in subhead 2 are met.

5. The communication to the data subject referred to in subhead 1 may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in Head 37.
Explanatory notes

This Head seeks to give effect to Article 31 (Communication of a personal data breach to the data subject) of the Directive.

Recital (62) reads inter alia:

"..... Where avoiding obstruction of official or legal inquiries, investigations or procedures, avoiding prejudice to the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protecting public security, protecting national security or protecting the rights and freedoms of others cannot be achieved by delaying or restricting the communication of a personal data breach to the natural person concerned, such communication could, in exceptional circumstances, be omitted."
Head 50 – Designation of data protection officer

Provide that:

1. Competent authorities shall designate a data protection officer; having regard to their structure and size, a single data protection officer may be designated for several competent authorities.

2. The data protection officer shall be designated on the basis of his or her expert knowledge of data protection law and practices and his or her ability to perform the tasks referred to in subhead 4.

3. Competent authorities shall—
   
   (a) ensure that the data protection officer is involved in an appropriate and timely manner in all matters relating to the protection of personal data,
   
   (b) support the data protection officer in performing the tasks referred to in subhead 4 by providing access to processing operations and the resources necessary to carry out these tasks;
   
   (c) assist the data protection officer in maintaining his or her expert knowledge in relation to data protection matters.

4. The tasks of the data protection officer shall include the following—
   
   (a) informing and advising the competent authority and staff members who are processing personal data of their obligations under this Part and other relevant Union or national law concerning data protection;
   
   (b) providing advice on awareness-raising activities, staff training, and the allocation of responsibilities in relation to data protection, as well as advising on and monitoring the carrying out of data protection impact assessments;
   
   (c) monitoring compliance with this Part and with other relevant Union or national law concerning data protection and with the policies of the controller in relation to the protection of personal data, including audit activity;
   
   (d) cooperating with the Commission and acting as a contact point for issues related to the processing of personal data, including prior consultation referred to in Head 46.
5. Competent authorities shall publish the contact details of the data protection officer and communicate them to the Commission.

**Explanatory notes**

This Head gives effect to Articles 32, 33 and 34; designation of data protection officers by competent authorities is mandatory under the Directive. Recital (63) reads:

*The controller should designate a person who would assist it in monitoring internal compliance with the provisions adopted pursuant to this Directive, except where a Member State decides to exempt courts and other independent judicial authorities when acting in their judicial capacity. That person could be a member of the existing staff of the controller who received special training in data protection law and practice in order to acquire expert knowledge in that field. The necessary level of expert knowledge should be determined, in particular, according to the data processing carried out and the protection required for the personal data processed by the controller. His or her task could be carried out on a part time or full time basis. A data protection officer may be appointed jointly by several controllers, taking into account their organisational structure and size, for example in the case of shared resources in central units. That person can also be appointed to different positions within the structure of the relevant controllers. That person should help the controller and the employees processing personal data by informing and advising them on compliance with their relevant data protection obligations. Such data protection officers should be in a position to perform their duties and tasks in an independent manner in accordance with Member State law.*

Article 32 also allows Member States to exempt courts and other independent judicial authorities when acting in their judicial capacity from the obligation to designate a data protection officer. This matter is covered in Part 5.
Chapter 4

Transfers of personal data to third countries or international organisations

Head 51 – Transfers to third countries or international organisations

Provide that:

1. Personal data may be transferred to a third country or an international organisation under this Part only if—
   
   (a) the transfer is necessary for purposes referred to in Head 27.1,
   
   (b) the personal data are transferred to a recipient in a third country or international organisation that is a competent authority for purposes referred to in Head 27.1,
   
   (c) subject to subhead 2, the competent authority in another Member State from which the personal data were obtained has given its prior authorisation to the transfer in compliance with its national law,
   
   (d) the third country or international organisation concerned ensures an adequate level of protection for the intended processing, and
   
   (e) in the case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer or another competent authority of the same Member State authorises the onward transfer after taking all relevant factors into account, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

2. Transfer without prior authorisation is permitted only if—
   
   (a) transfer of the personal data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State; and
   
   (b) such authorisation cannot be obtained in good time.

3. Where a transfer is made without prior authorisation, the competent authority responsible for giving it must be informed without delay.
4. For the purpose of subhead 1(d), a third country or international organisation is deemed to ensure an adequate level of protection for the intended processing where a decision (“adequacy decision”) in respect of that country or organisation for the purposes set out in Head 27.1 has been adopted by the European Commission by means of an implementing act under the examination procedure referred to in Article 58(2) of the Directive.

**Explanatory notes**

This Head gives effect to Article 35.1 and 2 of the Directive. Recital (64) reads inter alia:

…. A transfer should be carried out only by competent authorities acting as controllers, except where processors are explicitly instructed to transfer on behalf of controllers. ....

Recital (65) reads:

Where personal data are transferred from a Member State to third countries or international organisations, such a transfer should, in principle, take place only after the Member State from which the data were obtained has given its authorisation to the transfer. The interests of efficient law enforcement cooperation require that where the nature of a threat to the public security of a Member State or a third country or to the essential interests of a Member State is so immediate as to render it impossible to obtain prior authorisation in good time, the competent authority should be able to transfer the relevant personal data to the third country or international organisation concerned without such a prior authorisation. Member States should provide that any specific conditions concerning the transfer should be communicated to third countries or international organisations. Onward transfers of personal data should be subject to prior authorisation by the competent authority that carried out the original transfer. When deciding on a request for the authorisation of an onward transfer, the competent authority that carried out the original transfer should take due account of all relevant factors, including the seriousness of the criminal offence, the specific conditions subject to which, and the purpose for which, the data was originally transferred, the nature and conditions of the execution of the criminal penalty, and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred. The competent authority that carried out the original transfer should also be able to subject the onward transfer to specific conditions. Such specific conditions can be described, for example, in handling codes.

This Head builds on section 11(1) and (2) of the 1988 Act (as substituted by section 12 of the 2003 Act).
Head 52 – Transfers subject to appropriate safeguards

Provide that:

1. In the absence of an adequacy decision (see Head 51), a competent authority may transfer personal data to a third country or international organisation where—

   (a) appropriate safeguards with regard to the processing of personal data are provided for in a legally binding instrument, or

   (b) the competent authority has assessed all the circumstances surrounding the transfer and has concluded that appropriate safeguards exist with regard to the protection of the personal data.

2. Where personal data are transferred under subhead 1(b), the competent authority shall—

   (a) inform the Commission about categories of such transfers, and

   (b) keep a record, including details of the personal data, date and time of transfer, recipient and reasons for the transfer, and shall make it available to the Commission on request.

Explanatory notes

This Head gives effect to Article 37 of the Directive. Recital (71) reads inter alia:

.... Such legally binding instruments could, for example, be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and which could be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. The controller should be able to take into account cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. The controller should be able to also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, the controller should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, the controller should be able to require additional safeguards.

Section 11(4)(a)(ix) of the 1988 Act (as substituted by section 12 of the 2003 Act) allows for the transfer of personal data to third countries where the Data Protection Commissioner has authorised the transfer where the controller has adduced adequate safeguards.
Head 53 – Derogations for specific situations

Provide that:

1. In the absence of an adequacy decision or the appropriate safeguards referred to in Head 52, a transfer or a category of transfers of personal data to a third country or an international organisation may take place on condition that the transfer is necessary—
   (a) to protect the vital interests of a data subject or another person,
   (b) to safeguard legitimate interests of a data subject in accordance with national law,
   (c) for the prevention of an immediate and serious threat to public security of a Member State or a third country,
   (d) in individual cases for purposes set out in Head 27.1, or
   (e) in individual cases for establishment, exercise or defence of legal claims relating to purposes set out in Head 27.1.

2. In the case of transfers referred to in paragraphs (d) and (e) of subhead 1, personal data shall not be transferred if the competent authority considers that fundamental rights and freedoms of the data subject concerned override the public interest in making the transfer.

3. Where personal data are transferred under subhead 1, the competent authority shall keep a record, including details of the personal data, the date and time of transfer, the recipient and reasons for the transfer, and shall make it available to the Commission on request.

Explanatory notes

This Head gives effect to Article 38 of the Directive.

Similar derogations are set out in section 11(4) of the 1988 Act (as substituted by section 12 of the 2003 Act); this Head however reflects more closely the type of transfers that might be necessary in the context of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
Head 54 – Transfers to recipients in third countries

Provide that:

1. Notwithstanding Head 51.1(b) and without prejudice to any international agreement referred to in subhead 2, a competent authority may, in individual and specific cases, transfer personal data directly to a recipient established in a third country (“recipient”) only if other relevant provisions of this Part are complied with and the following conditions are fulfilled:

   (a) the transfer is strictly necessary for the performance of a task of the competent authority as provided for by Union law or national law for purposes set out in Head 27.1;

   (b) the competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case;

   (c) the competent authority considers that the transfer to a competent authority that is competent for the purposes referred to in Head 27.1 in the third country is ineffective or inappropriate, in particular because the transfer cannot be made in good time;

   (d) the competent authority that is competent for the purposes referred to in Head 27.1 in the third country concerned is informed of the transfer without undue delay, unless this is ineffective or inappropriate; and

   (e) the competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary.

2. An international agreement referred to in subhead 1 is any bilateral or multilateral international agreement in force between the State and a third country in the field of judicial cooperation in criminal matters and police cooperation.

3. The competent authority shall inform the Commission of transfers under this Head.

4. Where personal data are transferred under subhead 1, the competent authority shall keep a record, including details of the personal data, the date and time of transfer, the recipient and reasons for the transfer, and shall make it available to the Commission on request.
Explanatory notes

This Head gives effect to Article 39 of the Directive. Recital (73) reads:

Competent authorities of Member States apply bilateral or multilateral international agreements in force, concluded with third countries in the field of judicial cooperation in criminal matters and police cooperation, for the exchange of relevant information to allow them to perform their legally assigned tasks. In principle, this takes place through, or at least with, the cooperation of the authorities competent in the third countries concerned for the purposes of this Directive, sometimes even in the absence of a bilateral or multilateral international agreement. However, in specific individual cases, the regular procedures requiring contacting such an authority in the third country may be ineffective or inappropriate, in particular because the transfer could not be carried out in a timely manner, or because that authority in the third country does not respect the rule of law or international human rights norms and standards, so that competent authorities of Member States could decide to transfer personal data directly to recipients established in those third countries. This may be the case where there is an urgent need to transfer personal data to save the life of a person who is in danger of becoming a victim of a criminal offence or in the interest of preventing an imminent perpetration of a crime, including terrorism. Even if such a transfer between competent authorities and recipients established in third countries should take place only in specific individual cases, this Directive should provide for conditions to regulate such cases. Those provisions should not be considered to be derogations from any existing bilateral or multilateral international agreements in the field of judicial cooperation in criminal matters and police cooperation. Those rules should apply in addition to the other rules of this Directive, in particular those on the lawfulness of processing and Chapter V.
Chapter 5

Remedies, liability and penalties

Head 55 - Right to lodge a complaint with Commission

Provide that:

1. Without prejudice to any other available remedy, a data subject shall have the right to lodge a complaint with the Commission if he or she considers that processing of his or her personal data infringes this Part.

2. The Commission shall keep the data subject informed of progress made in dealing with the complaint and the outcome of any enquiry, investigation or procedure and the possibility of a judicial remedy under Head 91 [Part 6].

3. If the subject-matter of the complaint does not fall within the Commission’s competence, the Commission shall transmit it to the competent supervisory authority without undue delay and inform the data subject of the transmission.

4. Subhead 2 shall apply where the Commission receives a complaint from another supervisory authority and it is the competent supervisory authority.

Explanatory notes

This Head seeks to give effect to Article 52 of the Directive and builds on section 10 of the 1988 Act. Recital (85) reads inter alia:

Every data subject should have the right to lodge a complaint with a single supervisory authority and to an effective judicial remedy in accordance with Article 47 of the Charter where the data subject considers that his or her rights under provisions adopted pursuant to this Directive are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The competent supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be provided to the data subject.

It may be possible to incorporate this Head into Part 5 at the drafting stage.
Head 56 – Right to effective judicial remedy against Commission

Provide that:

1. Without prejudice to any other available remedy, a person may appeal against a legally binding decision of the Commission not later than 28 days after receiving the decision.

2. The Circuit Court shall, concurrently with the High Court, have jurisdiction to hear and determine proceedings under this Head.

3. An appeal under subhead 1 shall be determined by the court—
   
   (a) confirming the decision of the Commission, or
   
   (b) substituting its own determination for the Commission decision.

4. Without prejudice to any other available remedy, a data subject shall have the right to appeal to the Circuit Court where the Commission does not deal with a complaint which falls within the Commission’s competence or does not inform the data subject within three months of the progress or outcome of the complaint lodged under Head 55.

5. An appeal under subhead 4 shall be determined by the Circuit Court—

   (a) ordering the Commission to deal with the complaint or to inform the data subject of the progress or outcome of the complaint as the case may be, or

   (b) dismissing the appeal.

6. The jurisdiction conferred on the Circuit Court by this Head shall be exercised by the judge for the time being assigned to the circuit where the appellant ordinarily resides or the controller or processor is established.

7. A decision of the Circuit Court or High Court, as the case may be, shall be final save that, by leave of that Court, an appeal shall lie to the High Court or Court of Appeal, as the case may be, on a point of law.
8. For the purposes of this Head, a “legally binding decision” means a decision exercising the investigative or corrective powers of the Commission under Head 61 but excludes opinions issued or advice provided by the Commission.

**Explanatory notes**

This Head seeks to give effect to Article 53 of the Directive. The reference to “a person” in subhead 1 means that it includes a data subject, a controller, a processor or a third party (e.g. an individual other than the data subject affected by a decision of the Commission). Recital (86) reads:

> Each natural or legal person should have the right to an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, that right does not encompass other measures of supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with Member State law. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it.

Section 26 of the 1988 Act provides for appeals to the Circuit Court against decisions of the Data Protection Commissioner. Subhead 8 seeks to provide clarity in respect of a “legally binding” decision of the Commission in accordance with recital (86) of the Directive. It is intended that the content of this Head will be merged with that of Head 71 during the drafting process.
Head 57 – Representation of data subjects

Provide that:

1. A data subject shall have the right to mandate a body, organisation or association providing its services on a not-for-profit basis which—
   
   (a) has been properly constituted in accordance with law,

   (b) has statutory objectives which are in the public interest, and

   (c) is active with regard to the protection of data subject rights and freedoms, including protection of their personal data,

   to lodge a complaint on his or her behalf and to exercise the rights referred to in Heads 55 and 56 on his or her behalf.

2. Where the Commission or a court has reasonable doubts as to whether a body, organisation or association complies with the conditions referred to in subhead 1, it may request the provision of such additional information as is necessary in order to confirm such compliance.

Explanatory notes

This Head gives effect to Article 55 of the Directive. Recital (87) reads:

Where a data subject considers that his or her rights under this Directive are infringed, he or she should have the right to mandate a body which aims to protect the rights and interests of data subjects in relation to the protection of their personal data and is constituted according to Member State law to lodge a complaint on his or her behalf with a supervisory authority and to exercise the right to a judicial remedy. The right of representation of data subjects should be without prejudice to Member State procedural law which may require mandatory representation of data subjects by a lawyer, as defined in Council Directive 77/249/EEC, before national courts.
Head 58 – Right to compensation

Provide that:

A person who suffers material or non-material damage by reason of an infringement of this Part shall have the right to receive compensation from the competent authority or processor for damage or distress suffered

Explanatory notes

This Head seeks to give effect to Article 56 of the Directive.

Section 7 of the 1988 Act provides that a general duty of care in tort is to apply vis-a-vis the data controller and data subject. If, however, the data causes loss by virtue of inaccuracy and the data controller has obtained that data from a third party, the controller can avoid liability under this section in certain circumstances.
Chapter 6
Independent supervisory authority

Head 59 – Supervisory authority

Provide that:

1. The Commission shall be the supervisory authority for the purpose of this Part and the Directive and shall be responsible for monitoring the application of this Part on the territory of the State.

2. The Commission shall contribute to the consistent application of the Directive throughout the Union and for this purpose shall co-operate with other supervisory authorities and with the European Commission.


4. The Commission shall not be competent for the supervision of data processing by courts or other independent judicial authorities when acting in their judicial capacity.

Explanatory notes

Article 41 of the Directive requires Member States to designate a supervisory authority for the purposes of the Directive. This may be the supervisory authority established for the purposes of the GDPR. Subhead 4 gives effect to Article 45.2 (see Head 91).
Head 60 – Tasks of the Commission

Provide that:

1. For the purposes of this Part, the Commission shall—

   (a) monitor and enforce application of this Part and any implementing measures;

   (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;

   (c) advise, on request, the Houses of the Oireachtas, Government and public authorities and bodies on legislative proposals and administrative measures relating to the protection of individuals’ rights and freedoms with regard to data processing;

   (d) promote the awareness of competent authorities and processors of their obligations under this Part and the Directive;

   (e) provide, on request, information to data subjects on the exercise of their rights under this Part and, where appropriate, cooperate with other supervisory authorities for that purpose;

   (f) deal with complaints lodged by a data subject, or a body, organisation or association on his or her behalf, and investigate the complaint to the extent appropriate;

   (g) examine the lawfulness of processing pursuant to Head 28 and inform the data subject within a reasonable period of the outcome of the examination or of the reasons why the examination has not been carried out;

   (h) cooperate with and provide mutual assistance to other supervisory authorities with a view to ensuring consistent application and enforcement of the Directive;

   (i) conduct, on its own initiative or on the basis of information received from another supervisory authority or other public authority, investigations on the application of this Part;

   (j) monitor relevant developments insofar as they impact on the protection of personal data, in particular the development of information and communication technologies;

   (k) provide advice to a competent authority or processor, as the case may be, pursuant to Head 46; and

   (l) contribute to the activities of the European Data Protection Board.
2. Without excluding other means of communication, the Commission shall facilitate the submission of complaints referred to in subhead 1(f) by making a complaint form which can be completed electronically available on its web site.

3. Where the Commission investigates a complaint, it shall inform the data subject of the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary.

4. The Commission shall perform the tasks outlined in subhead 1 free of charge for data subjects and data protection officers.

5. Where the Commission receives a request which is manifestly unfounded or excessive, in particular because it is repetitive, it may impose a reasonable charge based on the administrative costs of responding to it or, alternatively, may refuse to act on the request; it shall be for the Commission to demonstrate that such a request is manifestly unfounded or excessive.

Explanatory notes
This Head gives effect to Article 46 of the Directive.
Head 61 – Powers of the Commission

Provide that:

1. For the purposes of this Part, the Commission shall have the following investigative powers:
   (a) to obtain from the competent authority and, where applicable, the processor, access to all personal data and to all information necessary for the performance of the tasks referred to in Head 60;
   
   (b) to order the competent authority and, where applicable, the processor to provide any information it requires for the purposes of responding to a complaint by or on behalf of a data subject;
   
   (c) to conduct audits for the purpose of ascertaining whether or not processing by a competent authority or processor is compliant with this Part.

2. For the purposes of this Part, the Commission shall have the following corrective powers:
   (a) to issue warnings to a competent authority or processor that intended data processing is likely to infringe this Part;
   
   (b) to issue reprimands to a competent authority or processor where data processing has infringed this Part;
   
   (c) to order a competent authority or processor to comply with a data subject’s request to exercise his or her rights;
   
   (d) to order a competent authority or processor to bring processing into compliance with this Part in a specified manner and within a specified period;
   
   (e) to order a competent authority to communicate a personal data breach to data subjects;
   
   (f) to impose a restriction on processing;
   
   (g) to order the suspension of data transfers to a recipient in a third country or to an international organisation.

3. The Commission shall have the power
   (a) to advise a controller or processor in accordance with the prior consultation procedure referred to in Head 46, and
(b) to issue opinions, on its own initiative or on request, on matters related to the protection of personal data to the Houses of the Oireachtas, Government, public authorities and bodies, as well as to the public.

Explanatory notes

This Head gives effect to Article 47 of the Directive. Subhead 2(e) gives effect to Article 31.4 of the Directive.

Subhead 2(b), (c) and (g) are inspired by Articles 58.2(b), (c) and (j) respectively of the General Data Protection Regulation. Moreover, the Data Protection Commissioner already has power to require a person to take such steps as are specified in order to comply with the Acts (section 10(2) of the Data Protection Act 1988), and power (subject to limitations) to prohibit the transfer of personal data to third countries (section 11(7) of the 1988 Act as substituted by section 11 of the Data Protection (Amendment) Act 2003). Recital (82) reads:

In order to ensure effective, reliable and consistent monitoring of compliance with and enforcement of this Directive throughout the Union pursuant to the TFEU as interpreted by the Court of Justice, the supervisory authorities should have in each Member State the same tasks and effective powers, including investigative, corrective, and advisory powers which constitute necessary means to perform their tasks. However, their powers should not interfere with specific rules for criminal proceedings, including investigation and prosecution of criminal offences, or the independence of the judiciary. Without prejudice to the powers of prosecutorial authorities under Member State law, supervisory authorities should also have the power to bring infringements of this Directive to the attention of the judicial authorities or to engage in legal proceedings. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards laid down in Union and Member State law, impartially, fairly and within a reasonable time. In particular, each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Directive, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure that would adversely affect the person concerned is taken, and avoiding superfluous costs and excessive inconvenience to the person concerned. Investigative powers as regards access to premises should be exercised in accordance with specific requirements in Member State law, such as the requirement to obtain a prior judicial authorisation. The adoption of a legally binding decision should be subject to judicial review in the Member State of the supervisory authority that adopted the decision.
Head 62 – Mutual assistance

Provide that:

1. The Commission shall provide other supervisory authorities with mutual assistance in order to ensure effective cooperation between them and to apply the provisions of the Directive in a consistent manner; it may involve responding to requests for information or undertaking supervisory measures such as the carrying out of consultations, inspections or investigations.

3. The Commission shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request.

3. Requests for mutual assistance shall contain all the necessary information, including the purpose of and reasons for the request; information exchanged shall be used only for the purpose for which it was requested.

4. The Commission shall not refuse to comply with a request unless:
   (a) it is not responsible for the subject-matter of the request or for the measures it is requested to carry out; or
   (b) compliance with the request would infringe Union or national law to which the Commission is subject.

The Commission shall provide reasons for any refusal to comply with a request to the requesting supervisory authority.

5. The Commission shall inform the requesting supervisory authority of the results of, or progress made in response to, a request.

6. As a general rule, the Commission shall supply information requested by other supervisory authorities by electronic means using a standardised format.
7. The Commission shall not charge a fee for any action taken in response to a request for mutual assistance.

8. The Commission may enter into an agreement with other supervisory authorities on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

**Explanatory notes**

This Head gives effect to Article 50 of the Directive. Section 15 of the 2008 Act already provides for mutual assistance in the context of Council of Europe Convention 108.
Exercise of supervision and enforcement powers by Data Protection Commission

1. The General Data Protection Regulation and this Act will confer important supervision and enforcement powers on supervisory authorities. The exercise of these powers must have regard to essential procedural safeguards, due process and judicial review.

2. Article 58 (Powers) of GDPR states in paragraph 4 that “The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter”. Article 83 (General conditions for imposing administrative fines) states in paragraph 8 that “The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union law and Member State law, including effective judicial remedy and due process.”

3. It is clear that the exercise of supervisory authority powers must be subject to “procedural safeguards” and “due process” in accordance with Union and Member State law. Consideration must therefore be given to these matters in the context of drafting this legislation.

4. The supervisory authority powers outlined in Article 58 of GDPR and Head 61 are potentially far reaching; moreover, the administrative fines outlined in Article 83 of GDPR are potentially massive. As regards the latter, the Regulation states that such fines “shall in each individual case be effective, proportionate and dissuasive”. It is likely that such potentially severe sanctions trigger application of Article 6 of ECHR and relevant case law of the Strasbourg court.

5. The foregoing points towards a need for robust procedural and due process safeguards (e.g. adequate notice; fair investigation and adjudication; opportunity to make submissions or oral hearing; need to give reasons for decisions).
Chapter 1 - General

Head 63 – Interpretation

Provide that:

1. In this Part, unless the context otherwise requires—

“business” in relation to a controller or processor means the controller’s or processor’s business as a controller or processor;

“controller” means a data controller or the data controller’s representative, and includes a competent authority;

“data equipment” means equipment for processing data;

“national law” includes a statute and an instrument made under a power conferred by a statute;

“enforcement notice” means a notice under Head 70;

“information notice” means a notice under Head 69;

“investigation report”, in relation to an investigation, means a report in writing prepared, following the completion of the investigation, by an authorised officer—

(a) stating that the authorised officer—
   (i) is satisfied that an infringement of the Regulation, this Act or regulations made under this Act by the controller or processor to which the investigation relates has occurred or is occurring, or
   (ii) is not so satisfied,

as appropriate,
(b) if paragraph (a)(i) is applicable, stating the grounds on which the authorised officer is so satisfied, and

(c) if paragraph (a)(ii) is applicable, stating—
   (i) the basis on which the authorised officer is not so satisfied, and
   (ii) the authorised officer’s opinion, in view of such basis, on whether or not a further investigation of the controller or processor is warranted and, if warranted, the authorised officer’s opinion on the principal matters to which the further investigation should relate;

“processor” means a data processor or the data processor’s representative;

2. A word or expression used in this Part and also in the Regulation or Directive has, unless the context otherwise requires, the same meaning in this Part as it has in the Regulation or Directive.

3. A reference to an Article, or part thereof, in this Part is, unless the context otherwise requires, a reference to an Article of the Regulation.

**Explanatory notes**

These are standard provisions.
Head 64 – Service of notice

Provide that:

1. A notice to be given to a controller or processor under this Act shall be given in one of the following ways:

   (a) by delivering it to the controller or processor;

   (b) by leaving it at the address at which the controller or processor ordinarily resides or carries on business;

   (c) by sending it by prepaid registered post or by any other form of recorded delivery service in an envelope addressed to the controller or processor at the address referred to in paragraph (b);

   (d) where the controller or processor has given an address for service of notices, by leaving it at the address for such service or sending it by prepaid registered post or by any other form of recorded delivery service in an envelope addressed to the controller or processor at that address; or

   (e) where, notwithstanding section 12(2)(c) of the Electronic Commerce Act 2000, the Commission considers that notice should be given electronically, by sending it by means of electronic mail to a device or facility for the reception of electronic mail located at the address at which the controller or processor ordinarily resides or carries on business or, if an address for the service of notices has been provided by the controller or processor, that address.

2. For the purposes of this Head, a company is deemed ordinarily resident at its registered office and every other body corporate or unincorporated body to be resident at its principal place of business.

Explanatory notes

This Head will replace section 25 of the 1988 Act.
Chapter 2 – Complaints and enforcement

Head 65 - Data subject complaints

Provide that:

1. Where a complaint is made to the Commission by or on behalf of a data subject [i.e. under Articles 77 or 80.1 or Head 55] that the processing of personal data relating to him or her infringes the Regulation or this Act, or regulations made under this Act, the Commission shall, to the extent that it considers appropriate, investigate the subject matter of the complaint or cause it to be investigated.

2. The Commission shall—
   (a) acknowledge receipt of such a complaint as soon as practicable and, in any event, no later than one month of receiving it,

   (b) inform the data subject of his or her right—
      (i) to be informed by the Commission within three months on the progress or outcome of the complaint,

      (ii) to apply to the Circuit Court under Head 71 in the event of a failure by the Commission to comply with subparagraph (i),

      (iii) to appeal under Head 71 against a legally binding decision of the Commission concerning him or her.

3. Where a complaint is withdrawn by or on behalf of a data subject, the Commission may proceed to investigate the complaint as if it had not been withdrawn if it is satisfied that there is good and sufficient reason for so doing; where the Commission proceeds as if a complaint had not been withdrawn, the investigation concerned shall be treated as an investigation initiated by the Commission.
4. Where the Commission has reasonable doubts concerning the identity of a complainant, the Commission may require the provision of such additional information as is necessary to confirm such identity.

**Explanatory notes**

The tasks of a supervisory authority under Article 57 of the Regulation include handling complaints lodged by or on behalf of data subjects under Articles 77 and 80 of the Regulation respectively. Likewise, the data subject may lodge a complaint under Part 4 (Head 55) and the Commission is tasked with handling such complaints under Head 60; investigative powers under Head 61 may be used for this purpose.

Subhead 3 is intended to allow the Commission to proceed with investigation of a complaint in cases in which the complaint has been withdrawn if there is good and sufficient reason for so doing.

The provision in subhead 4 is based on Article 12.6 of the GDPR (applicable to controllers). It will be possible to make on-line complaints and this may create problems for the Commission when it comes to establishing the identity of complainants.
Head 66 – Investigation and audit

Provide that:

1. The Commission may—

(a) to the extent appropriate, investigate or cause to be investigated, whether an infringement of the Regulation or this Act has occurred or is occurring where it is of opinion, for whatever reason, that there may be such an infringement [i.e. under Article 57.1(h) and Head 60.1(i)];

(b) carry out or cause to be carried out such examination in the form of an audit ("data protection audit") as it considers appropriate in order to determine whether the practices and procedures of a controller or processor are in compliance with the Regulation and this Act [Article 58.1(b) and Head 61.1(c)].

2. For the purposes of an investigation or audit, the Commission may require a controller or processor to produce any documents, records, statements or other information within that person’s possession or control, or within that person’s procurement, that are relevant to or required for investigation of a complaint or conduct of a data protection audit.

Explanatory notes

Article 58.1 of the Regulation confers investigative powers on the supervisory authority. The tasks of supervisory authorities under Article 58.1(b) also include investigations in the form of audits. Broadly similar tasks and powers are conferred on the Commission in Head 60 (Part 4).
Head 67 – Authorised officers

Provide that:

1. Where the Commission considers that it is necessary to do so for the purpose of the performance of its tasks or the exercise of its powers, it may appoint staff members or other suitably qualified persons to be authorised officers and to exercise any or all of the powers conferred by this Head.

2. A person appointed under subhead 1 shall, on his or her appointment, be furnished by the Commission with a certificate of his or her appointment and when exercising a power conferred by subhead 3 shall, if requested by any person thereby affected, produce such certificate together with a form of personal identification to that person for inspection.

3. An authorised officer may exercise any or all of the following powers—

   (a) enter, at any reasonable time, any premises or place where any activity connected with the processing of personal data or associated activity takes place or, in the opinion of the officer takes place, and search and inspect the premises or place and any documents, records, statements or other information found there,

   (b) require any person on the premises or at the place, being a controller or processor, or an employee or agent of either of them, to produce to him or her any documents or records relating to the processing of personal data or associated activity which are in that person’s power or control and, in the case of information in a non-legible form to reproduce it in a legible form, and to give to the officer such information as he or she may reasonably require in relation to any entries in such documents or records,

   (c) secure for later inspection—

      (i) any documents or records so provided or found and any data equipment, including any computer, in which those records may be held,
(ii) any such premises or place, or part thereof, in which documents, records or data equipment are kept or there are reasonable grounds for believing that such documents, records or data equipment are kept,

for such period as may reasonably be necessary for the purposes of the exercise of his or her powers;

(d) inspect and take extracts from or make copies of any such documents or records (including, in the case of information in a non-legible form, a copy of or extract from such information in a permanent legible form),

(e) remove and retain such documents or records for such period as may be reasonable for further examination or require any person referred to in paragraph (b) to maintain such documents or records for such period of time, as may be reasonable, as the authorised officer directs,

(g) require any person referred to in paragraph (b) to give to the officer any information which he or she may reasonably require with regard to the processing of personal data or associated activity and to afford the officer all reasonable assistance in relation thereto.

4. An authorised officer, in the exercise of any of his or her powers, may—

(a) operate any data equipment, including any computer, or cause any such data equipment or computer to be operated by a person accompanying the authorised officer, and

(b) require any person who appears to the authorised officer to be in a position to facilitate access to the documents or records stored in any data equipment or computer or which can be accessed by the use of that data equipment or computer to give the authorised officer all reasonable assistance in relation to the operation of the data equipment or computer or access to the records stored in it, including—
(i) providing the documents or records to the authorised officer in a form in which they can be taken and in which they are, or can be made, legible and comprehensible,

(ii) giving to the authorised officer any password necessary to make the documents or records concerned legible and comprehensible, or

(iii) otherwise enabling the authorised officer to examine the documents or records in a form in which they are legible and comprehensible

5. Where an authorised officer in exercise of his or her powers under this Head is prevented from entering any premises or place, an application may be made under Head 68 for a warrant to authorise such entry.

6. An authorised officer may require a person to provide him or her with his or her name and address where the authorised officer has reasonable grounds for requiring such information for the purpose of applying for a warrant under Head 68.

7. An authorised officer shall not, other than with the consent of the occupier, enter a private dwelling unless he or she has obtained a warrant under Head 68 authorising such entry.

8. A person to whom this Head applies who—

(a) obstructs, impedes or assaults an authorised officer in the exercise of a power under this Head,

(b) fails or refuses to comply with a requirement under this Head, including failure to provide the authorised officer with his or her name and address when requested to do so for the purpose of applying for a warrant under Head 68,

(c) alters, suppresses or destroys any documents, records, statements or other information which the person concerned has been required to produce, or may reasonably expect to be required to produce,
(d) gives to the authorised officer information, documents or records which the person knows to be false or misleading in a material respect,

(e) falsely represents himself or herself to be an authorised officer, or

(f) procures or seeks to procure any action referred to in paragraphs (a) to (e),

shall be guilty of an offence and liable—

(i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months, or both;

(ii) on conviction on indictment, to a fine not exceeding €250,000 or imprisonment for a term not exceeding 5 years, or both.

(9) An authorised officer appointed under section 24 of the Act of 1988 and holding office immediately before the commencement of this Head continues in office as if appointed under this Head [a transitional provision may be required here].

(10) The Commission may revoke an appointment made under subhead (1) or continued under subhead (9); such revocation shall be in writing.

(11) In this Head, “suitably qualified person” means a person other than a member of staff of the Commission who, in the Commission’s opinion, has the qualifications and experience necessary to exercise the powers conferred on an authorised officer by this Head.

Explanatory notes
This Head confers specific powers on authorised officers. It is based on the content of section 24 of the Data Protection Act 1988 and has been supplemented with additional provisions drawn from the Central Bank (Supervision and Enforcement) Act 2013. It would allow a staff member of another supervisory Authority to act as an authorised officer under joint operations arrangements (Article 62).
Head 68 – Search warrants

Provide that:

1. If a judge of the District Court is satisfied on the sworn information of an authorised officer that there are reasonable grounds for suspecting that information required by an authorised officer for the purpose of exercising his or her powers is held at any premises or place, the judge may issue a warrant authorising him or her, accompanied if the officer considers it necessary by such other person or a member of the Garda Síochána, at any time or times from the date of issue of the warrant, on production, if so required, of the warrant, to enter, if need be by reasonable force, the premises or place and exercise all or any of the powers conferred on an authorised officer under Head 67.

2. The period of validity of a warrant shall be 1 month from its date of issue but that period of validity may be extended in accordance with subheads 3 and 4.

3. The authorised officer may, during the period of validity of a warrant (including such period as previously extended under subhead 4), apply to a judge of the District Court for an order extending the period of validity of the warrant and such an application shall be grounded upon information on oath laid by the authorised officer stating, by reference to the purpose or purposes for which the warrant was issued, the reasons why the authorised officer considers the extension to be necessary.

4. If the judge of the District Court is satisfied that there are reasonable grounds for believing, having regard to that information so laid, that further time is needed so that the purpose or purposes for which the warrant was issued can be fulfilled, the judge may make an order extending the period of validity of the warrant by such period as, in the opinion of the judge, is appropriate and just; and where such an order is made, the judge shall cause the warrant to be suitably endorsed to indicate its extended period of validity.
5. Nothing in the preceding subheads prevents a judge of the District Court from issuing, on foot of a fresh application made under subhead 1, a further search warrant under this Head in relation to the same premises.

Explanatory notes
This Head is based on section 40 of the Communications Regulation Act 2002 and section 28 of the Central Bank (Supervision and Enforcement) Act 2013. There is no specific provision on these lines in the Data Protection Acts 1988 and 2003.
Head 69 – Power to require information (‘information notice’)

Provide that:

1. A Commissioner or an authorised officer may, by notice in writing (referred to in this Act as an “information notice”) served on a controller or processor, require the furnishing in writing within such time as may be specified in the notice and, if applicable in the format or manner specified in the notice, such information in relation to matters specified in the notice as is necessary or expedient for the performance by the Commissioner or authorised officer of the Commission’s functions.

2. An information notice shall state that the controller or processor concerned may seek a judicial remedy under Head 71 against the requirement specified in the notice within 28 days from service of the notice.

3(a). Nothing in this Head shall be taken to compel the furnishing by a controller or processor of documents, records, statements or other information which would be exempt from production in proceedings in a court on the ground of legal professional privilege.

(b) The controller or processor shall inform the Commission of any documents, records, statements or other information withheld under paragraph (a).

4. A controller or processor that, without reasonable excuse, fails or refuses to comply with a requirement specified in an information notice or who in purported compliance with such a requirement furnishes information to the Commissioner or authorised officer which the controller or processor knows to be false or misleading in a material respect shall be guilty of an offence and liable—

   (i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

   (ii) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.
5. A Commissioner or an authorised officer may cancel an information notice and, if it he or she does so, shall notify in writing the controller or processor on which it was served.

Explanatory notes
This Head, based on the ‘information notice’ procedure set out in section 12 of the Data Protection Act 1988, is intended to give effect to Article 58.1(a) of the Regulation which allows a supervisory authority to order a person (including a data controller, data processor or agent or representative of theirs) to provide any information required by the authority for the performance of its tasks.
Head 70 – Power to enforce (“enforcement notice”)

Provide that:

1. Without prejudice to Head 72, where a Commissioner or an authorised officer is of opinion that a controller or processor has contravened or is contravening the Regulation or this Act, or regulations made under Head 20 or Head 37, the Commissioner or authorised officer may, by notice in writing (referred to in this Act as an “enforcement notice”) exercise the Commission’s corrective powers under Article 58.2 or Head 61.2 requiring the controller or processor to take such steps as are specified in the notice within such time as may be so specified.

2. An enforcement notice shall—
   (a) specify the provision which, in the opinion of the Commissioner or authorised officer, has been or is being contravened and the reasons for having formed that opinion, and
   (b) state that the controller or processor concerned may seek a judicial remedy under Head 71 against the requirement specified in the notice within 28 days from service of the notice.

3. On compliance by a controller or processor with an enforcement notice, the controller or processor shall, as soon as may be and in any event not more than 28 days after such compliance, notify the steps taken to comply with the enforcement notice to—
   (a) the Commissioner or authorised officer concerned,
   (b) any data subject concerned, and
   (c) in the event of rectification or erasure of personal data or restriction of processing, any recipient to whom the data have been disclosed unless such notification proves impossible or involves a disproportionate effort; in such cases, the controller or processor shall also inform the data subject of the recipients if the data subject so requests.

4. A Commissioner or authorised officer may cancel an enforcement notice and, if he or she does so, shall notify in writing the controller or processor on which it was served.
5. Without prejudice to Article 83, a controller or processor who, without reasonable excuse, fails or refuses to comply with a requirement specified in an enforcement notice is guilty of an offence and liable—

(i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(ii) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

Explanatory notes

This Head is based on the enforcement notice procedure set out in section 10 of the Data Protection Act 1988.
Head 71 – Right to effective judicial remedy

Provide that:

1. An appeal by a controller or processor against a requirement specified in an information notice or enforcement notice shall be brought within 28 days from the service on the controller or processor, as the case may be, of the relevant notice.

2. An appeal against a legally binding decision of the Commission by a data subject or any other person affected by the decision shall be brought within 28 days of receiving the decision.

3. The Circuit Court shall, concurrently with the High Court, have jurisdiction to hear and determine proceedings under this Head.

4. An appeal under subhead 1 shall be determined by the court—
   (a) confirming the decision of the Commission, or
   (b) substituting its own determination for the Commission decision.

5. A data subject shall have the right to appeal to the Circuit Court where the Commission does not deal with a complaint which falls within the Commission’s competence or does not inform the data subject within three months of the progress or outcome of the complaint.

6. An appeal under subhead 5 shall be determined by the Circuit Court—
   (a) ordering the Commission to deal with the complaint or to inform the data subject of the progress or outcome of the complaint as the case may be, or
   (b) dismissing the appeal.

7. The jurisdiction conferred on the Circuit Court by this Head shall be exercised by the judge for the time being assigned to the circuit where the data subject resides or the controller or processor is established or, at the option of the controller or processor, by a judge of the Circuit Court for the time being assigned to the Dublin circuit.
8. A decision of the Circuit Court or High Court, as the case may be, shall be final save that, by leave of that Court, an appeal shall lie to the High Court or Court of Appeal, as the case may be, on a point of law.

9. For the purposes of this Head, a “legally binding decision” means a decision exercising the investigative or corrective powers of the Commission under Head 61 but excludes opinions issued or advice provided by the Commission.

Explanatory notes
This Head provides for appeals (1) by a data controller or data processor against an information notice or an enforcement notice issued by the Commissioner or an authorised officer, and (2) by a data subject against legally binding decisions of the Commission or where the Commission does not deal with a complaint which falls within the Commission’s competence or does not inform the data subject within three months of the progress or outcome of the complaint.
Head 72 – Exceptional circumstances in which application may be made to the High Court

Provide that:

1. Without prejudice to Article 66 and subhead 4, where the Commission considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects until steps or further steps are taken under the Regulation or this Act insofar as it gives further effect to the Regulation, it may, on notice to the controller or processor, as the case may be, make an application in a summary manner to the High Court for an order to suspend or restrict, as the case may be—
   (a) processing of personal data by such controller or processor,
   (b) transfer of personal data to a recipient in a third country or to an international organisation.

2. The High Court may determine an application under subhead 1 by—
   (a) making any order that it considers appropriate, including an order suspending or restricting—
      (i) the processing of personal data, or
      (ii) the transfer of such data to a recipient in a third country or an international organisation for such period, or until the occurrence of such event, as is specified in the order, and
   (b) giving to the Commission any other direction that the High Court considers appropriate.

3. The Commission shall, on complying with a direction of the High Court under subhead 2(b) give notice in writing to the controller or processor concerned of the Commission’s compliance with the direction.

4. Where the Commission considers that the immediate suspension or restriction of processing of personal data or transfer of such data to a recipient in a third country or an international organisation is necessary in order to protect the rights and freedoms of data subjects, it may
apply in a summary manner *ex parte* to the High Court for an interim order; the application shall be grounded on an affidavit sworn by or on behalf of the Commission.

5. (a) The High Court may make an interim order on an application under subhead 4 where, having regard to the circumstances of the case, the Court considers it necessary to do so for the protection of the rights and freedoms of data subjects.

   (b) If an interim order is made, a copy of the order and the affidavit referred to in subhead 4(b) shall be served on the controller or processor concerned as soon as is practicable.

   (c) The interim order shall have effect for a period, not exceeding 7 working days, to be specified in the order, and shall cease to have effect on the determination by the High Court of an application under subhead 1.

6 (a) An interim order under subhead 5 shall take effect on notification of its making being given to the controller or processor.

   (b) Oral communication to the controller or processor by or on behalf of the Commission of the fact that an interim order has been made, together with production of a copy of such order, shall, without prejudice to any other form of notification, be taken to be sufficient notification to the controller or processor concerned of the making of the order.

7. An application under subhead (4) shall be heard otherwise than in public unless the High Court considers it appropriate to hear the application in public.

8. The Commission shall communicate details of orders made by the High Court under this Head to the European Commission, European Data Protection Board and other supervisory authorities concerned.

**Explanatory notes**

Article 66 of the Regulation makes provision for an urgency procedure whereby provisional measures may be taken by the supervisory authority in order to protect the rights and freedoms of
data subjects. In such cases, the Commission is required to notify such measures, and the justification, to other concerned supervisory authorities, the European Commission and the European Data Protection Board. Where a provisional measure has been taken, and the Commission considers that final measures need to be adopted urgently, it may request an urgent opinion or binding decision of the European Data Protection Board.

This Head makes provision for a complementary national law mechanism along the lines of Article 66 that would allow the Commission to obtain a court order in cases of urgency. Article 58.4 permits the creation of additional supervisory authority powers in national law. The opportuneness of parallel mechanism will be discussed during drafting.
Head 73 – Power to require report

Provide that:

1. The Commission may for the purposes of proper and effective monitoring of application of the Regulation, and this Act insofar as it gives further effect to the Regulation, and having regard to the matters set out in subhead 3, by notice in writing to a controller or processor, require the controller or processor to provide to the Commission, in accordance with such notice, a report on any matter specified in the notice about which the Commission has required or could require the provision of information, or the production of any statement, record or document under any provision of the Regulation or this Act.

(2) A notice under subhead 1 shall be in writing and shall state—

(a) the date on which the notice was given,

(b) the period within which the controller or processor shall nominate a person to the Commission for approval under subhead 4,

(c) the purpose, scope and form of the report,

(d) the matters required to be reported on,

(e) the timetable for completion of the report,

(f) whether the report is to include recommendations,

(g) where appropriate, the methodology to be used in preparation of the report, and

(h) such other matters relating to the report as the Commission considers appropriate.

3. Before giving a notice under this Head, the Commission, taking account of the purpose for which the report is required, shall have regard to at least the following matters—

(a) whether any other powers that may be exercised by the Commission may be more appropriate in the circumstances concerned,

(b) the relevant knowledge and expertise available to the controller or processor, and

(c) the level of resources available to the controller or processor and the likely benefit to the controller or processor of providing the report.

4. A report required to be provided to the Commission under this Head shall be prepared by a person (referred to as the “reviewer”)—
(a) nominated by the controller or processor, within such period as is specified in the notice given under subhead 1, and approved by the Commission, or

(b) nominated by the Commission, where no person is nominated by the controller or processor within the period specified in the notice under subhead 1 or the Commission is not satisfied with the person so nominated.

5. When considering whether to approve a nomination under subhead 4(a) or make a nomination under subhead 4(b), the Commission shall have regard to the circumstances giving rise to the requirement for a report and whether the person it proposes to so approve or nominate as reviewer appears to have—

(a) the competence and expertise necessary to prepare the report,

(b) the ability to complete the report within the period specified by the Commission in the notice given under subhead 1,

(c) any relevant specialised knowledge, including specialised knowledge of the data processing activities carried on by the controller or processor and the matters to be reported on,

(d) any potential conflict of interest in reviewing the matters to be reported on,

(e) sufficient detachment, having regard to any existing professional or commercial relationship, to give an objective opinion, and

(f) any previous experience in preparing reports under this Head or reports of a similar nature.

6. Where the Commission approves a nomination under subhead 4(a) or makes a nomination under subhead 4(b) it shall notify the controller or processor, in writing, accordingly.

7. Where a reviewer is approved or nominated by the Commission under subhead 6, the controller or processor shall enter into a contract with the reviewer.

8. It shall be a term of the contract referred to in subhead 7—

(a) that the reviewer is required to prepare for the controller or processor a report in accordance with the notice given under subhead 1,

(b) that any duty owed by the reviewer to the controller or processor which might limit the provision of information or opinion by the controller or processor to the reviewer in preparing a report under this Head shall be waived,

(c) that the reviewer is required and permitted to provide to the Commission the following where the Commission so requests—
(i) periodic updates on progress and issues arising,

(ii) interim reports, and

(iii) copies of any draft reports given to the controller or processor.

9. If the Commission considers it appropriate, it may request the controller or processor to provide the Commission with a copy of the draft contract before it is made and the Commission may require such modifications to the draft contract as it considers appropriate.

10. The costs of and incidental to the preparation of a report under this Head shall be borne by the controller or processor.

11. A controller or processor shall give all such assistance to a reviewer as he or she may reasonably require for the purposes of the preparation of a report under this Head.

12. A reviewer shall, where requested by the Commission, in such form and within such period as the Commission may specify, provide an explanation of all or any part of a report under this Head or the recommendations, if any, made in the report, or of such other matters relating to the report as the Commission considers appropriate.

13. The Commission shall not be bound by the content of a report under this Head and such a report shall not be taken to be a decision or opinion of the Commission for any purpose.

14. The adoption by a controller or processor or any other person of a course of action recommended or described in a report under this Head does not represent an endorsement or approval of that course of action by the Commission.

15. The Commission shall not be liable for any acts or omissions of a reviewer or controller or processor relating to a report under this Part.

16. A person who—

(a) obstructs or impedes a reviewer in the preparation of a report under this Head,

(b) in relation to the preparation of a report under this Head, gives information to a reviewer that the person knows to be false or misleading in a material respect, or

(c) is a reviewer and in relation to the preparation of a report under this Head gives information to the Commission which the reviewer knows to be false or misleading in a material respect,

commits an offence and is liable—

(i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months, or both, or
(ii) on conviction on indictment, to a fine not exceeding €250,000 or imprisonment for a term not exceeding 5 years, or both.

Explanatory notes

Article 58.4 provides that Member States may provide that its supervisory authority shall have additional powers as long as they are consistent with the consistency mechanism in Chapter VII.

The Commission’s power to require submission of a report under this Head will provide it with an additional important instrument to obtain relevant information for the purposes of an investigation or audit of a controller or processor. The matters referred to in subhead are intended to ensure that the power is used in appropriate large-scale cases, taking account of the level of resources available to the controller or processor (subhead 10 imposes the costs of the report on the controller or processor concerned).

This Head is based on provisions in Part 2 of the Central Bank (Supervision and Enforcement) Act 2013.
Chapter 3 – Investigations

Head 74 – Investigations

Provide that:

1. Where the Commission decides that an investigation is justified in the circumstances of the case in order to ascertain whether an infringement of the Regulation or this Act has occurred or is occurring, the provisions of this Head shall apply.

2. The Commission may direct one or more authorised officers to conduct an investigation and to submit an investigation report to him or her.

3. The Commission may define the scope and terms of the investigation to be conducted, whether as respects the matters or the period to which it is to extend or otherwise, and may, in particular, limit the investigation to matters connected with particular circumstances.

4. As soon as is practicable after being appointed to conduct an investigation, the authorised officer shall—
   (a) if the investigation arises in consequence of a complaint lodged with the Commission—

   (i) cause notice in writing of the complaint to be given to the controller or processor to which the complaint relates, setting out particulars of the complaint, and

   (ii) afford to the controller or processor an opportunity to respond to the notice within 21 days from the date on which the notice was served (or such further period not exceeding 21 days as the authorised officer allows),

   (b) if the investigation has been initiated by the Commission other than in response to a complaint—

   (i) cause notice in writing to be given to the controller or processor concerned of the matters to which the investigation relates, and
(ii) afford to the controller or processor an opportunity to respond to the notice within 21 days from the date on which the notice referred to in subparagraph (i) was served (or such further period not exceeding 21 days as the authorised inspector allows).

Explanatory notes
This Head deals with the formalities of appointment an authorised officer to complete an investigation.
Head 75 – Power of investigation

Provide that:

1. For the purposes of an investigation, an authorised officer—
   
   (a) may require a controller or processor, or an employee or agent of either of them, that, in the authorised officer’s opinion—

   (i) possesses information that is relevant to the investigation, or

   (ii) has any statement, record, document or other information within that person’s possession or control or within that person’s procurement that are relevant to the investigation,

   to provide that information or statement, record, document or other information, as the case may be, to the authorised officer, and

   (b) where the authorised officer thinks fit, may require that controller or processor, or an employee or agent of either of them, to attend before him or her for the purpose of so providing that information or statement, record, document or other information, as the case may be, and the controller or processor shall comply with the requirement.

2. A requirement under subhead 1 shall specify—

   (a) a period within which, or a date and time on which, the controller or processor, or employee or agent of either of them, the subject of the requirement is to comply with the requirement, and

   (b) as the authorised officer concerned thinks fit—

   (i) the place at which the controller or processor, or employee or agent of either of them, shall attend to give the information concerned or to which the controller or processor, or employee or agent of either of them, shall deliver the statement, record, document or other information concerned, or
(ii) the place to which the controller or processor, or employee or agent of either of them, shall send the information or the statement, record, document or other information concerned.

3. A controller or processor, or employee or agent of either of them, required to attend before an authorised officer under subhead (2)—

(a) is also required to answer fully and truthfully any question put by the authorised officer and

(b) if so required by the authorised officer, shall answer any such question under oath.

4. Where it appears to an authorised officer that a controller or processor, or employee or agent of either of them, has failed to comply or fully comply with a requirement under subheads 2 or 3, the authorised officer may, on notice to that controller or processor and with the consent of the Commission, apply in a summary manner to the Circuit Court for an order under subhead 5.

5. Where satisfied after hearing an application under subhead 4 that the controller or processor, or employee or agent of either of them, has failed to comply or fully comply with the requirement in question, the Circuit Court may, subject to subhead 8, make an order requiring that person to comply or fully comply, as the case may be, with the requirement within a specified period.

6. An application under subhead 4 to the Circuit Court shall be made to a judge of that Court for the circuit in which the controller or processor has an establishment or, at the option of the controller or processor, by a judge of the Circuit Court for the time being assigned to the Dublin circuit.

7. The administration of an oath referred to in subhead 3(b) by an authorised officer is hereby authorised.

8. A controller or processor the subject of a requirement under subheads (1) or (3) shall be entitled to the same immunities and privileges in respect of compliance with such requirement as if the person were a witness before the High Court.
9. Any statement or admission made by a controller or processor pursuant to a requirement under subhead 1 or 3 is not admissible against that person in criminal proceedings other than criminal proceedings for an offence under subhead 13, and this shall be explained to the person in ordinary language by the authorised officer concerned.

10. Nothing in this Head shall be taken to compel the production by any controller or processor of statements, records or other documents which would be exempt from production in proceedings in a court on the ground of legal professional privilege.

11. For the purposes of an investigation, an authorised officer may, if he or she thinks it proper to do so, of his or her own volition conduct an oral hearing.

12. The Schedule shall have effect for the purposes of an oral hearing referred to in subhead 11.

13. Subject to subhead 10, a controller or processor which—
   (a) withholds, destroys, conceals or refuses to provide any information or statements, records or other documents required for the purposes of an investigation,

   (b) fails or refuses to comply with any requirement of an authorised officer under this Head, or

   (c) otherwise obstructs or hinders an authorised officer in the performance of functions imposed under this Act,

is guilty of an offence and liable—
   (i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

   (ii) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

14. In this Head, “documents, records and statements” include copies of statements or records.
Explanatory notes

This Head, based on subsections (3) to (17) of section 66 of the Property Services (Regulation) Act 2011, deals with the conduct of investigations by authorised officers. Any overlaps with Head 67.3 will be examined during drafting with a view to ensuring a coherent text.
Head 76 – Report of authorised officer

Provide that:

1. Where an authorised officer has completed an investigation, he or she shall, as soon as is practicable after having considered, in so far as they are relevant to the investigation—
   (a) any information, records or other documents provided to him or her,

   (b) any statement or admission made by any person,

   (c) any submissions made, and

   (d) any evidence presented (whether at an oral hearing or otherwise),

prepare a draft of the investigation report and give, or cause to be given, to the controller or processor to which the investigation relates—
   (i) a copy of the draft of the investigation report, and

   (ii) a notice in writing stating that the controller or processor concerned may, not later than 21 days from the date on which the notice was served on them (or such further period not exceeding 21 days as the authorised officer allows), make submissions in writing to the authorised officer on the content of the draft of the investigation report.

2. An authorised officer who has complied with subhead 1 shall, as soon as is practicable after—
   (a) the expiration of the period referred to in subhead 1(ii), and

   (b) having—

   (i) considered the submissions (if any) made before the expiration of that period on the draft of the investigation report concerned, and
(ii) made any revisions to the draft of the investigation report which, in the opinion of the authorised officer, are warranted following such consideration,

prepare the final report and submit it to a Commissioner with any such submissions annexed to it.

3. Where an authorised officer states, whether in a draft of the investigation report or in the final report, that he or she is satisfied that an infringement of the Regulation or this Act by the controller or processor to which the investigation relates has occurred or is occurring, the authorised officer shall not make any recommendation, or express any opinion, in such report as to the sanction that he or she considers ought to be imposed on the controller or processor in respect of such infringement in the event that the Commissioner is also satisfied that an infringement has occurred or is occurring.

Explanatory notes

This Head outlines the procedure to be followed following completion of an authorised officer’s report and its submission to the Commission.
Chapter 4 – Sanctions

Head 77 – Action arising from investigation report

Provide that:

1. When a Commissioner has considered an investigation report (and any submissions annexed to it) and he or she is the competent supervisory authority pursuant to Article 55 or 56.2, the Commissioner—

   (a) if he or she considers that further investigation is warranted, shall direct the authorised officer to conduct such further investigation into such matters as the Commissioner considers necessary having regard to the investigation report,

   (b) if satisfied that an infringement of the Regulation or this Act by the controller or processor to which the investigation relates has not occurred or is not occurring, and the investigation arose from a complaint, shall make a decision dismissing the complaint;

   (c) if satisfied that an infringement of the Regulation or this Act by the controller or processor to whom the investigation relates has occurred or is occurring, shall, subject to subhead (2) make a decision imposing such administrative fine or such enforcement notice, or both, on the controller or processor, as he or she thinks fit in the circumstances of the case.

2. Where the Commissioner has considered an investigation report (and any submissions annexed to it), the Commissioner may, if he or she considers that further information is required for the purpose of enabling him or her to make a decision under subhead (1)—

   (a) conduct an oral hearing if he or she considers that it is the most appropriate manner in which to obtain any further information required for such a decision, or

   (b) give to the controller or processor to which the investigation concerned relates—
(i) a copy of the investigation report, and

(ii) a notice in writing stating that the controller or processor may, not later than 21 days from the date on which the notice was served on them (or such further period not exceeding 21 days as the Commissioner allows), each make submissions in writing to the Commissioner in relation to the matters specified in the notice.

3. The Schedule shall, with any necessary modification, have effect for the purposes of an oral hearing referred to in subhead 2(a).

4. The Commissioner shall, as soon as is practicable after making a decision under subhead 1, give notice in writing of the decision and the reasons for it to the controller or processor to whom the investigation relates and, where subhead (1)(c) applies, set out in that notice details of the administrative fine or enforcement notice, or both.

5. The Commissioner shall, when determining any administrative fine to be imposed, have regard to the matters referred to in Article 83.2 of the Regulation.

6. Where subhead 4 applies in the case of an investigation which arose from a complaint, the Commissioner shall inform the complainant of the outcome of the investigation at the same time as the notice is given to the controller or processor, or as soon as is practicable thereafter.

**Explanatory notes**

The procedure set out in subheads 1 to 6 apply to straightforward domestic cases, i.e. cases in which there is no cross-border dimension involved and the Commissioner is acting as competent supervisory authority under Article 55 or Article 56.1.
**Head 78 - Cooperation and consistency mechanism**

**Provide that:**

1. Where the Commission is acting as lead supervisory authority under Article 56.1 of the Regulation, the Commissioner shall prepare a draft decision instead of the decision referred to in Head 77 and shall submit it to other supervisory authorities concerned for their opinion.

2. In the absence of a relevant and reasoned objection, the draft decision shall be adopted by the Commissioner in accordance with Head 77(1)(b) or (c), as the case may be.

3. Where one or more of the supervisory authorities concerned expresses a relevant and reasoned objection to the draft decision within four weeks of having been consulted, the Commissioner shall take due account of any views expressed and—

   (a) if he or she is not minded to revise the draft decision in response to an objection or is otherwise of the opinion that an objection is not relevant or reasoned, refer the draft decision to the Board pursuant to Article 65.1(a) of the Regulation;

   (b) if he or she is minded to revise the draft decision in response to an objection, revise the draft decision, submit it to the other supervisory authorities concerned for their opinion and shall take due account of any views expressed pursuant to Article 60.3.

4. In the event of a further relevant and reasoned objection, the dispute shall be resolved by the Board in accordance with Article 65 of the Regulation.

5. Following receipt of notification of the decision of the Board, the Commissioner shall, on the basis of the Board’s decision, adopt his or her final decision, including any enforcement notice or

---

2 Defined in Article 4 of the Regulation.
3 Defined in Article 4 of the Regulation.
administrative fine, and give notice in writing of it, and the reasons for it to the controller or processor.

**Explanatory notes**

Whereas the previous Head deals with ‘domestic’ cases (i.e. there is no cross-border dimension involved), a much more complex procedure must be followed in cases of cross border processing cases (one-stop-shop) cases (defined in Article 4).

In such cases, the Commission’s draft decision must be submitted to other “concerned” supervisory authorities for their views and the Commission must “take due account of their views”. If the Commission, for whatever reason, is not minded to take due account of any such views (for example, they may be without merit, or there may be conflicting views which cannot be reconciled), the draft decision must be referred to the European Data Protection Board acting as a dispute resolution mechanism under Article 65. Where differences of approach persist, the dispute falls to be resolved by the European Data Protection Board under Article 65.
Head 79 – Appeal against administrative fine

Provide that:

1. Without prejudice to Head 71, a controller or processor the subject of a decision by a Commissioner under Head 77.1(c) or Head 78.5 to impose an administrative fine may, not later than 30 days from the date on which notice of the decision was served, appeal to the court against the decision.

2. The court may, on hearing an appeal under subhead 1, consider any evidence adduced or argument made by the controller or processor, whether or not already adduced or made to an authorised officer or Commissioner.

3. Subject to subhead 4, the court may, on the hearing of an appeal under subhead (1)—
   (a) confirm the decision the subject of the appeal,
   (b) replace it with such other decision as the court considers just and appropriate, including a decision to impose a different fine or no fine, or
   (c) annul the decision.

4. The court shall, for the purposes of subhead (3)(b) have regard to the matters referred to in Article 83.1 and 2 of the Regulation.

5. In this Head, “the court” means—
   (a) the High Court, or
   (b) the Circuit Court when exercising the monetary jurisdiction in civil proceedings conferred on it under the Courts and Civil Law (Miscellaneous Provisions) Act 2013.

6. The jurisdiction conferred on the Circuit Court by this Head shall be exercised by the judge for the time being assigned to the circuit where the data subject resides or the controller or processor is established or, at the option of the controller or processor, by a judge of the Circuit Court for the time being assigned to the Dublin circuit.
Explanatory notes

This Head allows for appeals against administrative fines imposed by the Commission for infringements of the Regulation. The appeal may be brought before the Circuit Court where the fine amounts to less than €75,000.
Head 80 – Circuit Court to confirm decision to impose administrative fine

Provide that:

1. Where a controller or processor concerned does not appeal to the court against a decision by the Commission under 77.1(c) or 78.5 to impose an administrative fine within the period allowed under Head 79, the Commission shall, as soon as is practicable after the expiration of that period and on notice to the controller or processor, make an application in a summary manner to the Circuit Court for confirmation of the decision.

2. The Circuit Court shall, on the hearing of an application under subhead 1, confirm the decision the subject of the application unless the Court sees good reason not to do so.

3. The jurisdiction conferred on the Circuit Court by this Head shall be exercised by the judge for the time being assigned to the circuit where the controller or processor is established or, at the option of the controller or processor, by a judge of the Circuit Court for the time being assigned to the Dublin circuit.

Explanatory notes
This Head, based on section 71 of the Property Services (Regulation) Act 2011, provides for confirmation of an administrative fine, irrespective of the level of fine, by the Circuit Court (the 2011 Act provides for confirmation of sanctions by the High Court but this appears to be excessive in the absence of any appeal against the fine imposed). The operation of this mechanism will be discuss further with the European Commission.

The words in subhead 2 “unless the Court sees good reason not to do so” is similar to those used in section 76(3) of the Medical Practitioners Act 2007. The manner in which they should be interpreted is outlined by Kelly P in his recent High Court ruling in The Medical Council – v – MAGA [2016] IEHC 779. In short, it does not mean that the court sits as a court of appeal but rather as a mechanism to ensure that a decision is taken in line with procedural rules and constitutional justice (paragraphs 30 and 31). It may be useful to explain this further rather than rely on the words “unless the Court sees good reason not to do so” which give no indication of the Court’s role..
Head 81 – Unauthorised disclosure by processor.

Provide that:

1. Personal data processed by a processor shall not be disclosed by the processor or by an employee or agent, without the prior authority of the controller on behalf of whom the data are processed.

2. A person who knowingly or recklessly contravenes subhead 1 shall be guilty of an offence and liable—

   (i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

   (ii) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

Explanatory note

Article 28 of the Regulation makes provision for a detailed contract between the controller and processor to be put in place; the controller can seek damages for any breach of the contract. However, Article 28.10 also makes reference to possible penalties under Article 84. This Head reproduces the existing section 21 of the 1988 Act. It specifically prohibits disclosure by a processor or sub-processor of person data without the prior authority of the data controller and makes such disclosure an offence.
Head 82 – Disclosure of personal data obtained without authority.

Provide that:

1. A person who—
   (a) obtains or procures access to personal data, or obtains any information constituting such data, without the prior authority, whether express or implied, of the controller or processor by whom the data are kept, and
   (b) discloses the data or information to another person,
   shall be guilty of an offence and liable—
   (i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or
   (ii) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.

2. Subhead 1 does not apply to a person who shows that the obtaining, disclosing or procuring was—
   (a) necessary for the purpose of preventing or detecting an offence,
   (b) required or authorised by or under any enactment, rule of law or order of a court, or
   (c) in the particular circumstances, justified as being in the public interest.

3. A person who sells or offers to sell personal data obtained in contravention of subhead 1 shall be guilty of an offence and liable—
   (i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or
   (ii) on conviction on indictment, to a fine not exceeding €50,000 or imprisonment for a term not exceeding 5 years or both.
Explanatory notes

This Head is based on section 22 of the 1988 Act. It criminalises, for example, hacking into personal data, or obtaining of such data by means of ‘blagging’, i.e. managing to obtain personal data illegally by using persuasion or guile. A number of cases of this nature have been successfully prosecuted by the Data Protection Commissioner in the recent years. Subhead 2 sets out exceptions to the general rule; subparagraph (b) draws inspiration from section 55 of the UK Data Protection Act 1998.

Subhead 3 seeks to combat the sale of illegally-obtained personal data by creating a new offence; it draws inspiration from section 55(4) and (5) of the UK’s 1998 Act.
Head 83 – Offences by directors etc. of bodies corporate

Provide that:

Where an offence under this Act is committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, a person being a director, manager, secretary or other officer of the body corporate or a person who was purporting to act in any such capacity, that person, as well as the body corporate, is guilty of that offence and is liable to be proceeded against and punished accordingly.

Explanatory notes
This Head reproduces the content of section 29 of the Data Protection Act 1988.
Head 84 – Prosecution of summary offences by Commission

Provide that:

1. Summary proceedings for an offence under this Act may be brought and prosecuted by the Commission.

2. Notwithstanding subsection 10 (4) of the Petty Sessions (Ireland) Act 1851, summary proceedings for an offence under this Act may be brought—
   (a) at any time within 3 years from the date on which the offence was alleged to have been committed, or
   (b) if, at the expiry of that period, the person against whom the proceedings are to be brought is outside the State, within 6 months of the date on which he or she next enters the State,
whichever is the later, provided that no such proceedings shall be commenced later than 5 years from the date on which the offence concerned was alleged to have been committed.

3. Where a person is convicted of an offence under this Act, the court shall, unless it is satisfied that there are special and substantial reasons for not so doing, order the person to pay the costs and expenses, measured by the court, incurred by the Commission in relation to the investigation, detection and prosecution of the offence, including the expenses of and incidental to an examination of any information provided to the Commissioner or an authorised officer.

4. An order for costs and expenses under subhead 3 is in addition to and not instead of any fine or other penalty the court may impose.

Explanatory notes
Subheads 1 and 2 are based on the content of section 30 of the 1988 Act; the extended period in subhead 2 is derived from section 55(2) of the Central Bank (Supervision and Enforcement) Act 2013. Subheads 3 and 4 are based on section 57 of the same Act.
Head 85 – Publication of convictions, sanctions etc.

Provide that:

1. The Commission shall publish particulars, in such form and manner and for such period as it thinks fit, of any—
   (a) conviction of a person for a contravention of this Act,
   (b) exercise of his or her corrective powers—
      (i) to impose an administrative fine [Article 58.2(i)], or
      (ii) to order the suspension of data transfers to a recipient in a third country or to an international organisation [Article 58.2(j)].

2. The Commission may publish particulars, in such form and manner and for such period as it thinks fit, of the exercise of its corrective powers under Article 58.2 or Head 61.2.

3. The Commission may, if it considers it appropriate to do so, publish particulars of any report by the Commission of any investigation or audit carried out, or other function performed, by it under the Regulation or this Act, or any matter relating to or arising in the course of such an investigation, audit or performance.

4. The publication by the Commission of particulars of any report or matters referred to in subhead 3 and any other report of the Commission, including its annual report, shall be absolutely privileged for the purposes of the law of defamation.

Explanatory note
This Head requires the Commissioner to publish details of convictions, the imposition of administrative fines and any suspensions of data transfers. A broadly similar provision is in section 91 of the Property Services (Regulation) Act. Subhead 3 is based on section 47(3) of the Freedom of Information Act 2014. Subhead 4 is based on section 14(3) of the 1988 Act.
Chapter 5 – Miscellaneous

Head 86 – Privileged legal material

Provide that:

1. Where a controller or processor refuses to produce information, or provide access to it, on the grounds that the information contains privileged legal material, a Commissioner or authorised officer may, at any time within 28 days of such refusal, apply to the High Court for a determination as to whether the information, or any part of the information, is privileged legal material where—

   (a) in relation to the information concerned—

   (i) the Commissioner or authorised officer has reasonable grounds for believing that it is not privileged legal material, or

   (ii) due to the manner or extent to which such information is presented together with any other information, it is impossible or impractical to extract only such information,

   and

   (b) the Commissioner or authorised officer has reasonable grounds to suspect that the information contains evidence relating to an infringement of the Regulation or this Act.

2. A controller or processor referred to in subhead (1) who refuses to produce information or provide access to it on the grounds that the information contains privileged legal material shall preserve the information and keep it in a safe and secure place and manner pending the determination of an application under subhead (1) and shall, if the information is so determined not to be privileged legal material, produce it in accordance with such order as the Court considers appropriate.
3. A person shall be considered to have complied with the requirement under subhead (2) to preserve information where the person has complied with such requirements as may be imposed by an authorised officer under paragraph (c) of Head 67(3).

4. Where an application is made by the Commissioner or authorised officer under subhead 1, the High Court may give such interim or interlocutory directions as it considers appropriate including, without prejudice to the generality of the foregoing, directions as to the appointment of a person with suitable legal qualifications possessing the level of experience and independence from any interest falling to be determined between the parties concerned, that the Court considers to be appropriate for the purpose of—

   (a) examining the information, and

   (b) preparing a report for the Court with a view to assisting or facilitating the Court in the making of its determination as to whether the information is privileged legal material.

5. An application under subhead 1 shall be by motion and may, if so directed, be heard otherwise than in public.

6. In this Head, “privileged legal material” means information which, in the opinion of the High Court, a person is entitled to refuse to produce on the grounds of legal professional privilege.

**Explanatory notes**

This Head is intended to provide a Commissioner or authorised officer with a remedy in cases in which a data controller or data processor refuses to provide information or access to it on grounds that it contains privileged legal material but the Commission has reasonable grounds for believing that it does not contain such material but rather evidence relating to an infringement of data protection legislation [see Head 69.3 (a) and (b)].
Head 87 – Presumptions

Provide that:

1. The presumptions specified in this section shall apply in any proceedings under the Regulation or this Act.

2. Where a document purports to have been created by a person it shall be presumed, unless the contrary is shown, that the document was created by that person and that any statement or record contained in it, unless the document expressly attributes its making to some other person, was made by that person.

3. Where a document purports to have been created by a person and addressed and sent to a second person, it shall be presumed, unless the contrary is shown, that the document or record was created and sent by the first person and received by the second person, and that any statement or record contained in it—
   (a) unless the document or record expressly attributes its making to some other person, was made by the first person, and
   (b) came to the notice of the second person.

4. Where a document or record is retrieved from an electronic storage and retrieval system, it shall be presumed, unless the contrary is shown, that the author of the document is the person who ordinarily uses that electronic storage and retrieval system in the course of his or her business.

5. Where an authorised officer who, in the exercise of his or her powers, has removed one or more documents or records from any premises or place, gives evidence in any proceedings that, to the best of his or her knowledge and belief, the material is the property of any person, then the material shall be presumed, unless the contrary is shown, to be the property of that person.

6. Where, in accordance with subhead (5), material is presumed in proceedings to be the property of a person and the authorised officer concerned gives evidence that, to the best of his or her knowledge and belief, the material is material which relates to any trade, profession, or, as the case...
may be, other activity, carried on by that person, the material shall be presumed, unless the contrary is proved, to be material which relates to that trade, profession, or, as the case may be, other activity, carried on by that person.

7. References in this Head to a document or record are references to a document or record in written, mechanical or electronic form and, for this purpose “written” includes any form of notation or code whether by hand or otherwise and regardless of the method by which, or medium in or on which, the document or record concerned is recorded.

**Explanatory notes**

This Head is based on section 12 of the Competition Act 2002. There is no equivalent provision in the Data Protection Acts 1988 and 2003.
Head 88 – Expert evidence

Provide that:

1. In any proceedings under the Regulation or this Act, the opinion of any witness who appears to possess the appropriate qualifications or experience as respects the matter to which his or her evidence relates shall, subject to subhead 2, be admissible in evidence as regards any matter calling for expertise or special knowledge that is relevant to the proceedings and, in particular and without prejudice to the generality of the foregoing, the following matters, namely—

   (a) the effects that types of data processing such as profiling may have, or have had, on the protection of personal data,

   (b) an explanation of any relevant practices or the application of such practice, where such an explanation would assist the proceedings.

2. Notwithstanding subhead 1, a court may, where in its opinion the interests of justice require it to so direct in the proceedings concerned, direct that evidence of a general or specific kind referred to in the said subhead shall not be admissible in proceedings or shall be admissible in such proceedings for specified purposes only

Explanatory notes

This Head recognises that expert assistance and evidence may be required in the course of any proceedings because of the technical complexity of certain data processing operations (e.g. use of cookies) and the complex structure of some business models (e.g. cloud computing). It is based on section 9 of the Competition Act 2002.
Head 89 – Immunity from suit

Provide that:

Civil or criminal proceedings shall not lie in any court against a Commissioner, authorised officer or a member of the staff of the Commission in respect of anything said or done in good faith by the Commissioner, authorised officer or member of staff in the course of the performance or purported performance of a function of the Commissioner, authorised officer or member of staff.

Explanatory notes

This Head is based on section 49(4) of the Freedom of Information Act 2014; there is no equivalent provision in the Data Protection Acts 1988 and 2003. A right of action shall, however, lie against the Commission.
Part 6 – Miscellaneous provisions

Head 90 – Supervisory authority for courts acting in judicial capacity

Provide that:

1. The judge for the time being assigned for that purpose by the Chief Justice shall be competent for supervision of data processing operations of the courts when acting in their judicial capacity.

2. The assigned judge shall, in particular—
   (a) promote awareness of data protection rules among judges and ensure compliance with them,
   (b) handle, and investigate to the extent appropriate, complaints in relation to data processing operations of the courts when acting in their judicial capacity.

3. The scope of rights and obligations provided for in—
   (a) Articles 12 to 22 and 34 of the Regulation (as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22),
   (b) Sections _ to _ [i.e. sections giving effect to Articles (11), 12, 13, 14, 16 and 31 of the Directive, as well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in these Articles]

may be restricted by rules of court to the extent necessary and proportionate in a democratic society in order to safeguard—
   (i) the protection judicial independence and judicial proceedings, and
   (ii) the enforcement of civil law claims

Explanatory notes

Article 55.3 of the Regulation and Article 45 of the Directive both provide that supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity. Recital (20) of the Regulation states, however, that “It should be possible to entrust supervision of such processing operations to specific bodies within the judicial system”. Moreover, Article 8.3 of the Charter of Fundamental Rights requires that compliance with data
protection rules be subject to control by an independent authority. The European Commission takes the view that Member States are required to establish a specific mechanism in order to comply with the Regulation.

The content of this Head is the subject of ongoing consultations with the Courts Service.

Subhead 1 provides for the assignment by the Chief Justice of a judge to act as supervisory authority for courts when acting in their judicial capacity. Subhead 2 specifies tasks that are mentioned in recital (20) of the Regulation.

Article 23 of the GDPR permits, by means of a legislative measure, restrictions on the exercise of data subject rights which are necessary and proportionate in a democratic society in order to safeguard important objectives of general public interest, including, specifically, the protection of judicial independence and judicial proceedings. The Directive allows similar flexibility.

Subhead 2 provides that such restrictions on the exercise of data subject rights may be specified in court rules. It is likely that the statutory terms of reference of Rules Committees will have to be broadened to include the making of rules in respect of the exercise of data subject rights.
Head 91 - Judicial remedy

Provide that:

1. Where a data subject considers that his or her rights under the Regulation or this Act have been infringed as a result of processing of his or her personal data, such infringement shall be actionable at the suit of the data subject ("data protection action").

2. The Circuit Court shall, concurrently with the High Court, have jurisdiction to hear and determine proceedings under this Head.

3. In a data protection action under this Head, the Circuit Court shall, without prejudice to its powers to award compensation in respect of material or non-material damage, have the power to grant relief by means of injunction or declaratory orders.

4. For the purpose of commencing a data protection action, the data subject shall, in particular, specify—
   (a) particulars of the acts of the controller or processor constituting the alleged infringement, and
   (b) any material or non-material damage alleged to have been occasioned by the infringement.

5. The jurisdiction conferred on the Circuit Court by this Head may be exercised by the judge of the circuit in which—
   (a) the controller or processor has an establishment, or
   (b) the data subject has his or her habitual residence except where the controller or processor is a public authority of the State acting in the exercise of its public powers.

Explanatory notes

Article 79 of the Regulation and Article 54 of the Directive require establishment of a “parallel” avenue of redress through the courts whereby, without prejudice to any other administrative or non-judicial remedy (including the right to lodge a complaint with the Commissioner), a data subject will have a right to an effective judicial remedy.
The court processes must in any event be used where a data subject seeks compensation for material or non-material damage under Article 82 of the Regulation or Article 56 of the Directive (Head 3.35) irrespective of whether or not he or she has already lodged a complaint with the Data Protection Commissioner.

Provision is made elsewhere in this Bill for appeals to the Circuit Court against decisions of the Data Protection Commissioner and appeals of Circuit Court decisions to the High Court on points of law.
Head 92 - Rules of court for data protection actions

Provide that:

1. It shall be the function of the courts in data protection actions to ensure that parties to such actions comply with such rules of court as apply in relation to such actions so that the trial of data protection actions within a reasonable period of their having been commenced is secured.

2. Where rules of court prescribe a period of time for the service of a document, or the doing of any other thing, in relation to a data protection action, the period within which that document may be served or thing may be done, shall not be extended beyond the period so prescribed unless—

   (a) the parties to the action agree to the period being extended, or

   (b) the court considers that—

   (i) in all the circumstances the extension of the period by such further period as it may direct is necessary or expedient to enable the action to be properly prosecuted or defended, and

   (ii) the interests of justice require the extension of the period by that further period.

3. For the purposes of ensuring compliance by a party to a data protection action with rules of court, a court may make such orders as to the payment of costs as it considers appropriate.

4. Nothing in this Head shall be construed as limiting or reducing the power of an authority, having (for the time being) power to make rules regulating the practice and procedure of a court, to—

   (a) make such rules in relation to data protection actions provided such rules do not derogate from, and are not inconsistent with, any provision of the Regulation, or

   (b) make such rules in relation to proceedings or actions other than data protection actions.

5. In subheads 1 and 2, a reference to the courts or the court includes a reference to the Master of the High Court and a county registrar.
Explanatory notes

It would be undesirable for large numbers of claims arising from alleged infringements of the Regulation or this Act to remain pending before the courts. This Head is, therefore, modelled on section 9 of the Civil Liability and Courts Act 2004.
Head 93 - Legal privilege

Provide that:

The rights and obligations provided for in—

(a) Articles 12 to 22 and 34 of the Regulation (as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22),

(b) Sections _ to _ [i.e. sections giving effect to Articles (11), 12, 13, 14, 16 and 31 of the Directive, as well as Article 4 in so far as its provisions correspond to such rights and obligations]

do not apply—

(i) to personal data processed for the purpose of seeking, receiving or giving legal advice (legal advice privilege),

(ii) 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, including personal data consisting of communications between a client and his or her legal advisers or between those advisers (litigation privilege),

(iii) where the exercise of such rights or performance of such obligations would constitute a contempt of court.

Explanatory notes

This Head seeks to protect legal privilege to the extent necessary and proportionate in a democratic society.
Head 94 - Amendment of section 33AK of Central Bank Act 1943

Provide that

Section 33AK (5) of the Central Bank Act 1942 is amended by inserting the following after paragraph (az):

“(--) to the Data Protection Commission that is required for the exercise of that Commission’s powers under the Data Protection Acts.”

Explanatory notes

Section 33AK(5) of the 1942 Act the Central Bank may disclose confidential information to a recipient on condition that such recipient does not disclose it if such disclosure is prohibited by the Rome Treaty, the ESCB statute or the supervisory EU legal acts. Article 90 of the Regulation allows Member States to adopt specific rules in relation to controllers or processors that are subject to an obligation of professional secrecy or other equivalent obligation of secrecy.

The inclusion of this Head has been recommended by the Central Bank.
Head 95 – Application to refer case to the CJEU

Provide that

1. Where, notwithstanding an implementing act pursuant to Article 45.3 of the Regulation or Article 36.3 of the Directive, the Commission considers that a third country, a territory or one or more specified sectors within a third country, or an international organisation, to which personal data are to be transferred does not ensure an adequate level of protection within the meaning of Article 45.2 of the Regulation or 36.2 of the Directive, it may apply to the High Court for—

   (a) a determination as to whether the level of protection is adequate, or

   (b) an order referring the matter to the Court of Justice for preliminary ruling under Article 267 TFEU.

2. Where, notwithstanding the adoption of standard data protection clauses pursuant to Article 46.1(c) or (d), the Commission is of the opinion that they do not ensure an adequate level of protection, it may apply to the High Court for—

   (a) a determination as to whether the level of protection is adequate, or

   (b) an order referring the matter to the Court of Justice for preliminary ruling under Article 267 TFEU.

Explanatory Notes

Chapter V (Transfers of personal data to third countries or international organisations) specifies the rules for transfer of personal data from the EU to third countries and international organisations.

Article 45 provides, inter alia, that:

(1) A transfer of personal data to a third country or international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

(2) The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 24 of this Article. …..

4 Paragraph 2 sets out a non-exhaustive list of the issues to be taken into account when assessing the adequacy of the level of protection.
(3) The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

(9) Decisions adopted by the Commission on the basis of article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 of 5 of this Article.

Article 46 provides inter alia:

(1) In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

(2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(c) standard data protection clauses adopted by the Commission pursuant to the examination procedure referred to Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to Article 93(2);

(4) .... Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Directive (EU) 2016/680 contains a provision on the lines of Article 45.

Court of Justice case law
In Schrems v Data Protection Commissioners, the CJEU held that under Article 288 TFEU, a Commission decision under Article 25(6) [of the 1995 Directive] is “binding on all the Member States to which it is addressed and is therefore binding on all their organs” until such time as the decision is withdrawn, annulled or declared invalid. It went on to say that only the CJEU could annul such a decision or declare it invalid following a reference for a preliminary ruling or a plea of illegality. It then noted that the independent supervisory authorities are vested with the power to check whether data transfers from the EU to third countries comply with the requirements laid down by the 1995 Directive even where the Commission had adopted an adequacy decision.

When a supervisory authority is asked to examine a complaint about the adequacy of the level of protection in a third country which is the subject of an adequacy decision, the Court noted that it may consider that the complaint is unfounded or well founded. If it considers the claim unfounded and rejects it, the person who lodged the claim must have access to judicial remedies enabling him or her to challenge such a decision before national courts. The court must then stay the

5 Case C-2015/650
proceedings and make a reference for preliminary ruling to the CJEU where it considers the claim well founded. On the other hand, if the supervisory authority considers the complaint well founded, that authority must have the possibility to engage in legal proceedings:

“... It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision’s validity.”

Further consideration will be required in relation to the scope of this provision, the form of application, and the available reliefs.
Provide that:

1. The authorised officer conducting an oral hearing under Head 75.11 for the purposes of an investigation may take evidence on oath, and the administration of such an oath by the authorised officer is hereby authorised.

2. The authorised officer may by notice in writing require a controller or processor to attend the oral hearing at such time and place as is specified in the notice to give evidence in respect of any matter in issue in the investigation or to produce any documents, records statements or other information within his or her possession or control or within his or her procurement.

3. Subject to subhead 4, a controller or processor referred to in subhead 2 may be examined and cross-examined at the oral hearing.

4. A controller or processor referred to in subhead 2 shall be entitled to the same immunities and privileges in respect of compliance with any requirement referred to in that paragraph as if the person were a witness before the High Court.

5. Where a controller or processor referred to in subhead 2 does not comply or fully comply with a requirement referred to in that subhead, the authorised officer may apply in a summary manner to the Circuit Court, on notice to that person, for an order requiring the person to comply or fully comply, as the case may be, with the requirement within a period to be specified by the Court, and the Court may make the order sought or such other order as it thinks fit or refuse to make any order.

6. The jurisdiction conferred on the Circuit Court by subhead 5 may be exercised by the judge of that Court for the circuit in which the person concerned ordinarily resides or has an establishment.

7. The oral hearing shall be held otherwise than in public.