Tithe an Oireachtais

An Comhchoiste um Dhlí agus Ceart agus Comhionannas

Tuarascáil maidir leis an nGrinnscrúdú Réamhreachtach ar Scéim Ghinearálta an Bhille um Chosaint Sonraí 2017

Samhain 2017

Houses of the Oireachtas

Joint Committee on Justice and Equality

Report on pre-legislative scrutiny of the General Scheme of the Data Protection Bill 2017

November 2017

32/JAE/7

Contents

Chairman's Preface

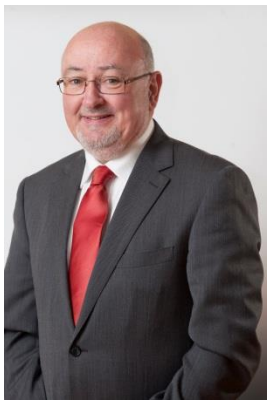
The issue of data protection has become a prescient one in the digital age, as people conduct more tasks online. Ireland is positioned as a fulcrum of activity for multinational technology corporations, and must therefore ensure that stringent data protection regulations are in place to protect its citizens. Data protection involves a number of complex components, and must strike a balance between, on the one hand, allowing enterprises and public bodies to function effectively, and on the other, the right of citizens to privacy.

The Committee therefore heard expert evidence from a range of stakeholders on the provisions of the General Scheme of the Data Protection Bill 2017. The Committee also sought written submissions on the issue from a number of stakeholders.

The General Data Protection Regulation will grant significant rights to all citizens in Ireland, but will provide particular protections to children. The Committee has recommended that an appropriate digital age of consent for children is set, and that this age be reviewed as technology evolves. The Committee has also recommended that children be consulted on data protection provisions to ascertain their views on the legislation, and that educational programmes be enacted to empower them to stay safe online.

A copy of this report and recommendations has been sent to the Minister for Justice and Equality. The Committee hopes it will assist and inform the drafting of the eventual Bill itself.

I would like to express my gratitude on behalf of the Committee to all the witnesses who attended our public hearings to give evidence. Finally, I also wish to thank the staff of the Committee Secretariat, and of the Library & Research Service, who assisted in the preparation of this report. Go raibh maith agaibh.



Caoimhghín Ó Caoláin T.D.
Chairman – November 2017

1. Introduction

The General Scheme of the Data Protection Bill (May 2017) ('General Scheme') was published by the Department of Justice and Equality on 12 May 2017.[1] The purpose of the proposed legislation is to:

- give further effect to the EU General Data Protection Regulation ('GDPR');
- transpose Directive (EU) 2016/680 ('Law Enforcement Directive'); and
- re-establish the Data Protection Commissioner as the Data Protection Commission and propose a number of procedural provisions concerning the operation of the Commission.

• Pre-legislative scrutiny by the Committee

On 16 May 2017, the then Minister for Justice and Equality, Frances Fitzgerald, TD, requested the Oireachtas Joint Committee on Justice and Equality ('Committee') to consider the General Scheme in terms of pre-legislative scrutiny ('PLS').

As part of its scrutiny of the Draft Heads of the General Scheme, the Committee met in public session on 14 June, 21 June and 5 July 2017.

The following stakeholders appeared before the Committee on 14 June 2017:

- Officials from the Department of Justice and Equality; and
- Representatives from the Office of the Data Protection Commissioner ('DPC').

The following stakeholder appeared before the Committee on 21 June 2017:

- Denis Kelleher, barrister-at-law.

The following stakeholders appeared before the Committee on 5 July 2017:

- Representatives from Digital Rights Ireland ('DRI'); and
- Dr Geoffrey Shannon, Special Rapporteur on Child Protection.

• Report structure

This report is divided into eight sections: An introduction (section 1), followed by seven sections focussing on the following themes:

[1] Available at: http://www.justice.ie/en/JELR/Pages/PR17000155

- **Summary of key issues (section 2)** – this section will summarise the key issues explored in the report.
- **Background (section 3)** – this section will provide an overview of, and background to, the General Scheme.
- **Structure of data protection law (section 4)** – this section will look at stakeholders' recommendations concerning the repeal of existing data protection law and the structure of the proposed legislation.
- **Children's rights and data protection (section 5)** - this section will look at the proposed legislation from the context of children's rights including stakeholders' recommendations concerning the proposed digital age of consent and the holding of consultations with children regarding the proposed legislation.
- **Sanctions (section 6)** - this section will look at the proposals for applying administrative fines on public bodies acting as an undertaking and an individual's right to receive compensation under the GDPR. It will also look at the possibility for representation by not-for-profit bodies on behalf of data subjects and 'class actions'.
- **Restrictions to the rights and obligations in the GDPR (section 7)** – this section will look at stakeholders' recommendations concerning the proposal in the proposed legislation to permit the restriction of specified rights and obligations set down in the GDPR where it is necessary to "safeguard important objectives of general public interest".
- **Performance information scrutiny on the General Scheme of the Data Protection Bill (May 2017) (section 8)** – this section proposes some potential indicators that may assist in performance scrutiny of the legislation after its enactment.

This report identifies the most pertinent broad themes treated by the General Scheme. The identification of key issues is based on an analysis from secondary sources and submissions and statements made to the Committee.

2. Executive summary of key issues

Key issues are summarised below in the order in which they occur in the main body of this report. The key issues are grouped into the themes highlighted in sections 4 to 7 of the report.

1. Structure of data protection law (section 4)

Head 5 of the General Scheme, entitled "Repeals", proposes to repeal the *Data Protection Act 1988*[2] and the *Data Protection (Amendment) Act 2003*[3] ('*Data Protection Acts*').[4] However, Head 5 is blank. Thus, it is not clear from Head 5 if the *Data Protection Acts* will be repealed in their entirety.

Key issues 1 - 4: Structure of data protection law

The Data Protection Commissioner ('the Commissioner') stated that it should be possible to identify which pieces of the *Data Protection Acts* are not a result of EU data protection law, and to repeal and re-enact those provisions in separate legislation. The Commissioner noted that a piecemeal approach to data protection law in Ireland could be perceived as a lack of commitment to the new data protection regime and be damaging to the State's and the Commissioner's reputation.

While Dr Denis Kelleher (Barrister-at-Law) agreed with the Commissioner that a piecemeal approach to data protection law in Ireland would not be desirable, he expressed concerns for reasons of timeliness as to the feasibility of repealing the *Data Protection Acts* in their entirety. In particular, that the legislation giving further effect to the GDPR must be in place by 25 May 2018. He queried if a drafting solution could allow for their repeal and re-enactment at a later date.

Dr TJ McIntyre (representative from Digital Rights Ireland) stated the *Data Protection Acts* should be repealed in their entirety. Dr McIntyre also recommended that the Law Enforcement Directive is transposed in a separate piece of legislation and to help avoid confusion that the GDPR should be annexed or appended to the proposed legislation.

Key issue 1: Repeal of the *Data Protection Acts*

Consideration should be given to repealing the *Data Protection Acts* in their entirety. It would be desirable in the interest of clarity that any provisions of the *Data Protection Acts* that fall outside the scope of EU data protection law but need to be retained in national law such as the provisions relating to *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* would be repealed and re-enacted in separate stand-alone legislation.

However, if repealing the existing *Data Protection Acts* in their entirety is not possible at this time, consideration should be given to finding a drafting solution whereby the proposed legislation acts as an entirely new stand-alone Data Protection Act, leaving behind a separate or distinct part(s) of the *Data Protection Acts* whose repeal and re-enactment could be addressed at a later date.

Key issue 2: Structure of the proposed legislation

[2] Available at: http://www.irishstatutebook.ie/eli/1988/act/25/enacted/en/html
[3] Available at: http://www.irishstatutebook.ie/eli/2003/act/6/enacted/en/html
[4] An administrative consolidated version of the Data Protection Acts (updated to 7 April 2017) is available on the Law Reform Commission website here: http://revisedacts.lawreform.ie/eli/1988/act/25/front/revised/en/html

Data protection is a nuanced and complex area which will continue to grow in complexity as more data protection law is enacted at the EU level and through case law. There is merit in giving consideration to the feasibility of transposing the Law Enforcement Directive in separate legislation. This may also allow for the full repeal of the *Data Protection Acts* as it may present an opportunity to address the repeal and re-enactment of any necessary remaining provisions at that time.

Key issue 3: Structure of the proposed legislation

The core aims of the GDPR are transparency and the strengthening of EU citizens' rights in the area of data protection and empowering them to exercise their rights. To aid in achieving these core aims, consideration should be given to reproducing verbatim the text of the GDPR in the proposed legislation as an annex or appendix.

Key issue 4: Structure of the proposed legislation

Following the enactment of the proposed legislation, consideration should be given to producing an administrative consolidated version of the GDPR with the corresponding national law provisions. This will result in individuals only having to read through one document when ascertaining their data protection rights and obligations. This would make data protection law more accessible and aid the safeguarding of citizens' fundamental right to protection of their personal data.

2. Children's rights and data protection (section 5)

Dr Geoffrey Shannon's (Special Rapporteur on Child Protection) evidence focussed specifically on the following children's rights issues:

(i) the digital age of consent;
(ii) the need for certain definitions relating to children and data protection;
(iii) the right to be forgotten;
(iv) the link between data protection and digital safety; and
(v) the processing of sensitive personal data.

- **Digital age of consent**

Head 16 of the General Scheme, entitled "*Child's consent in relation to information society services [Article 8]*", proposes to set down the digital age of consent for Ireland. Head 16 is blank as to the digital age of consent.

The Irish Times reported that on 26 July 2017, the Cabinet agreed that the digital age of consent should be set at 13 years of age.

Key issue 5: Digital age of consent

Evidence from children's rights organisations, and their advocates, were in agreement that the digital age of consent should be set at 13 years of age. The Cabinet subsequently agreed, on 26 July 2017, that the digital age of consent should be set at 13 years of age.

Dr Mary Aiken (cyber-psychologist) and Mr O'Sullivan (Professor, Department of Computer

Science, University College Cork), responding in The Irish Times to the recommendation that the digital age of consent should be set at 13 years of age, called for the digital age of consent to be set closer to 16 rather than 13 years of age.

After the enactment of the proposed legislation, there is merit in reviewing the digital age of consent that has been set by the Legislature as part of the post enactment scrutiny of the Bill to ensure that the age that has been set is, in practice, in the best interests of children.

- **Consultation with children**

Article 3 of the United Nations Convention on the Rights of the Child (UNCRC) provides that children have the right to have their best interest treated as the primary interest in all matters affecting him or her. Article 12 of the UNCRC provides that "children who are capable of forming their own views enjoy the right to express these views freely in matters affecting them and that due weight be given to them".

Key issue 6: Consultation with children

Evidence from Dr Shannon and the Ombudsman for Children emphasised the importance of giving children the opportunity to express their views, and have those views taken into account, on the parts of the proposed legislation that affect children.

Dr Shannon stated that it was unclear if children had been consulted on aspects of the proposed legislation that will affect them. He recommended that "a consultation process takes place to ascertain the views of a variety of age groups of children on the issue of digital consent".

Consideration should be given to carrying out a consultation process with children to give them the opportunity to express their views, and have those views taken into account, on the parts of the proposed legislation that affect children. Such consultation should include a variety of age groups of children.

- **Definitions**

Neither the GDPR nor the General Scheme defines 'children' or 'child'.

Key issue 7: Definition of the 'child'

The Ombudsman for Children recommended the proposed legislation provide a definition for 'child' and the definition, in keeping with the definition of 'child' in Article 1 of the UNCRC, should include every human being below 18 years of age.

In the interest of clarity, consideration should be given to providing in the proposed legislation a definition of 'child' and the definition should include every human being below 18 years of age.

Head 16 concerning the digital age of consent provides that consent is required from 'the holder of parental responsibility' for children below the digital age of consent. The General Scheme does not define 'the holder of parental responsibility'.

Key issue 8: Definition of 'the holder of responsibility'

Dr Shannon stated that the term 'the holder of responsibility' used in Head 16 of the General Scheme is not defined in Irish law. Noting the enhanced rights for a large number of citizens with respect to children and families under the *Children and Family Relationships Act 2015*, he recommended that the term is defined and that the definition should include any parent and guardian of the child, whether automatic or court appointed.

In the interest of clarity, consideration should be given to providing in the proposed legislation a definition of the term 'holder of parental responsibility' and such definition should be broadly defined to include any parent and guardian of the child, whether automatic or court appointed.

Recital (38) of the GDPR provides that "the consent of the holder of parental responsibility for the child should not be necessary in the context of "preventative or counselling services offered directly to a child". Neither the GDPR nor the General Scheme defines 'preventative or counselling services'.

Key issue 9: Definition of the 'preventative or counselling services'

Dr Shannon stated it is not clear whether the range of preventative or counselling services offered to children will fall within the scope of 'preventative or counselling services'. He recommended the proposed legislation provide a definition for 'preventative or counselling services' and that the definition should be defined in the broadest possible manner so children can avail of support when they need it.

Given the above, consideration should be given to providing in the proposed legislation a definition of 'preventative or counselling services', and such definition should be broadly defined so children can avail of support when they need it.

- **Right to be forgotten and children**

There is no provision in the General Scheme giving effect to the right to be forgotten as provided for in Article 17 of the GDPR. Head 35 of the General Scheme, entitled '*Right to rectification, erasure or restriction of processing*', transposes the right to be forgotten for the purposes of Article 16 of the Law Enforcement Directive only.

Key issue 10: Right to be forgotten and children

Dr Shannon emphasised the importance of the right to be forgotten (Article 17 of the GDPR) in the context of children. He noted that the General Scheme does not give effect to the right to be forgotten as provided for in the GDPR nor does it provide for an accompanying procedure for 'taking-down' personal data from the internet.

The Ombudsman for Children stated provisions in the proposed legislation concerning the right to rectification and the right to be forgotten (Article 16 of the Law Enforcement Directive) should explicitly reference children and young people's rights in this regard.

There is merit in considering whether the right to be forgotten, alongside the procedure for 'taking-down' personal data from the internet, should be explicitly provided for in the parts of the proposed legislation giving effect to the GDPR. In particular, whether they should be

provided for in respect of children.

Where the right to rectification and the right to be forgotten are explicitly provided for in the proposed legislation, consideration should be given to making an explicit reference to children and young people's rights in this regard.

- **Link between data protection and digital safety**

Key issue 11: Policy framework and educational programme to assist children in exercising their digital rights before they reach the digital age of consent

Dr Shannon stated that more needs to be done in Ireland to, firstly, empower young people to understand the benefits and downsides of the online world and, secondly, adult data literacy.

Dr Mary Aiken (cyber-psychologist) and Mr O'Sullivan (Professor, Department of Computer Science, University College Cork), commenting in The Irish Times on evidence from stakeholders during PLS hearings on the General Scheme, stated that Ireland needs to put in place a policy framework and an associated educational programme that ensures that children are sufficiently aware and responsible in order to understand and exercise their digital rights by the time they reach the digital age of consent.

Consideration should be given to developing and putting in place a policy framework, and an associated educational programme, to help empower children to understand the benefits and downsides of the online world and to improve adult data literacy in order to improve digital safety for children.

- **Processing sensitive personal data of children**

Head 17 of the General Scheme entitled "*Processing of special categories of personal data for reasons of substantial public interest [Article 9.2(g)*" proposes to grant the Minister discretionary power, by Regulations, to permit the processing of special categories of personal data for reasons of "substantial public interest". Such Regulations are to "respect the essence" of the right to data protection and contain "suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject".

Head 18 of the General Scheme, entitled "*Processing of special categories of personal data [Article 9.2 (b), (h), (i) and (j) and 4]*", proposes that the categories of sensitive data listed in Head 18(1) may be processed where necessary for, among other matters, "the management of health and social care systems and services and for public interest reasons in the area of public health." The processing of such data are to be "[s]ubject to suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject".

The Explanatory Notes to Head 18 of the General Scheme stated that there is uncertainty as to whether the "suitable and specific safeguards" are additional or complementary to the data controller obligations in the GDPR. The Explanatory Notes also stated the possibility of

including a 'toolbox' of possible safeguards in a new subhead that will be explored during drafting.

Key issue 12: Additional safeguards for the processing of sensitive personal data

Dr Shannon stated that consideration should be given to the inclusion of additional safeguards for the processing of sensitive personal data under Head 18 of the General Scheme, in particular where a child's sensitive personal data is involved and is to be processed.

There is merit in considering the inclusion of safeguards (additional to the safeguards provided for in the GDPR) in the proposed legislation where it avails of the derogation from the prohibition on processing sensitive personal data in Article 9 of the GDPR.

- **Provision of identification services**

Under Article 8(2) of the GDPR data controllers are required to "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".

Key issue 13: Provision of identification services

Dr Kelleher stated that under the GDPR there is a legal obligation to process personal data for the purposes of identifying persons ('identification services'). For example, social media organisations will have to be able to distinguish between adults and children. He questioned who is going to provide such services e.g. whether the State or private bodies will provide identification services. He noted that if the State is not providing identification services, the default position will be that private bodies will provide such services.

Dr Kelleher also explained that protective oversight for individuals will be different depending on who is providing identification services. He stated that if the State is, individuals will have many protective oversight options such as judicial review and fair procedures. However if private bodies are, protective oversight options available to individuals will be lower and will include either bringing a case to court or complaining to the DPC.

In light of Dr Kelleher's evidence, there is merit in giving consideration to, and possibly holding a public consultation on, whether the State or private bodies should provide identification services.

3. Sanctions (section 6)

- **Administrative fines**

Article 83 of the GDPR provides general conditions for the imposition of administrative fines by supervisory authorities for breaches of certain data protection laws. However, under Article

83(7) it is left to the discretion of Member States to set down rules on whether, and to what extent, administrative fines may be imposed on public authorities and bodies ('public bodies').

Head 23 of the General Scheme, entitled "*Imposition of administrative fines on public authorities and bodies (Article 83(7)),* proposes that administrative fines may be imposed on public bodies for data breaches arising from its activity as an "undertaking", e.g. where a public authority or body is providing a good or service alongside a private body, i.e. public and private hospital.

Key issue 14: Administrative fines

The Commissioner stated that "[i]t is a serious matter of concern" for the office that administrative fines would not be imposed on public bodies and that all organisations should be treated equally, regardless of whether they are engaged in commercial activity or any other activity. Not to do so would nullify the deterrent value of administrative fines in the public sector.

Mr Simon McGarr (representative of DRI) stated that there does not seem to be any reasons for exempting public bodies and recommended that Article 83(7) of the GDPR is implemented without any restrictions.

In view of the recommendation of the Data Protection Commissioner (DPC), and other stakeholders, that all public bodies should be capable of being subjected to administrative fines where they breach data protection protocols, consideration should be given to providing in the proposed legislation that all public bodies be subject to an administrative fine from the DPC for an infringement of data protection law.

- **Right to receive compensation**

Article 82 of the GDPR provides that a person who suffers material or non-material damage (i.e. where they suffered distress or humiliation) due to an infringement of the GDPR has a right to receive compensation from the data controller or data processor.

Although, Head 58 proposes to provide a right to compensation this is for the purposes of the Law Enforcement only. The General Scheme does make an explicit reference to the right to receive compensation for the purposes of the GDPR. However, Head 91 of the General Scheme, entitled '*Judicial remedy*', proposes that the infringement of a data subject's rights under the GDPR or the proposed legislation "shall be actionable at the suit of the data subject ("data protection action")".

Head 91(3) proposes to provide that "[i]n a data protection action under this Head, the Circuit Court shall, without prejudice to its powers to award compensation in respect of material and non-material damage, have the power to grant relief by means of injunction or declaratory orders."

Key issue 15: Right to receive compensation

Mr Seamus Carroll (official from the Department of Justice and Equality) stated that the Department are still reviewing a number of policy issues. In addition, consultations with the European Commission, the Attorney General's Office and the Data Protection Commissioner are on-going, including matters relating to compensation.

Dr Kelleher queried whether an explicit provision concerning the right to receive compensation for the purposes of the GDPR was needed in the proposed legislation.

Mr McGarr and Dr Eoin O'Dell (Associate Professor, School of Law, Trinity College Dublin) stated that the use of "shall" in Article 82 of the GDPR indicates that a Member State is required to give full effect to the provision.

Mr McGarr and Dr O'Dell similarly stated that Head 91 of the General Scheme recognises, or assumes, a right of action before the courts, but does not provide an explicit right to compensation. They cautioned that the failure by the State to give explicit recognition to the right to receive compensation could leave the State open to claims for damages from individuals. Each recommended the proposed legislation give explicit recognition to the right to receive compensation under both the Law Enforcement Directive and the GDPR.

In view of the evidence given to the Committee, that Ireland may need to explicitly provide a right to receive compensation in respect of the GDPR, consideration should be given to whether the proposed legislation should explicitly provide a right to receive compensation for the purposes of the GDPR. There is merit in directly addressing this issue as part of its on-going consultations with the DPC, the Office of the Attorney General and the European Commission.

- **Representation of data subjects by not-for-profit bodies and 'class actions' for data protection beaches**

Article 80 of the GDPR concerning representation of data subjects provides that the data subjects "shall have the right to mandate a not-for-profit body, organisation or association", meeting certain conditions, to lodge a complaint and exercise their rights under Articles 77 (the right to lodge a complaint with the supervisory authority), 78 (the right to an effective judicial remedy against the supervisory authority) and 79 (the right to an effective judicial remedy against a data controller or data processor) of the GDPR.

Article 80 of the GDPR also provides that Member States "may provide" that not-for-profit bodies have the right to lodge a complaint in that Member State with the data protection authority independently of a data subject's mandate, where it considers that a data subjects rights under the GDPR have been infringed.

Key issue 16: Representation by not-for-profit bodies, organisations or associations in data protection actions

Dr McIntyre stated that Article 80 of the GDPR contains one mandatory provision requiring Member States to permit individuals to nominate not-for-profit bodies to lodge a complaint on

his or her behalf. The General Scheme is silent as to this obligation.

Dr McIntyre also stated that Article 80 of the GDPR has two discretionary provisions that Member States may:

- permit individuals to mandate not-for-profit bodies to seek damages on his or her behalf; and
- provide that not-for-profit bodies can independently bring actions without having to be mandated by an individual data subject to do so.

The General Scheme is silent as to these two discretionary provisions in Article 80 of the GDPR.

Dr McIntyre highlighted practical and principled reasons for implementing these two discretionary provisions. These include that there would be "a multiplicity of claims being brought...that the courts simply are not equipped to address" and that it may result in a gap in the implementation of data protection law.

Consideration should be given to providing in the proposed legislation that an individual can mandate a properly qualified not-for-profit body, organisation or association, on the data subject's behalf, to lodge a complaint and to exercise their rights under Articles 77 (the right to lodge a complaint with the supervisory authority), 78 (the right to an effective judicial remedy against the supervisory authority) and 79 (the right to an effective judicial remedy against a data controller or data processor) of the GDPR.

There is also merit in giving consideration to providing in the proposed legislation that individuals may mandate a properly qualified not-for-profit body, organisation or association to seek compensation on his or her behalf.

In addition, there is also merit in giving consideration to providing that a properly qualified not-for-profit body, organisation or association can independently bring actions that there have been breaches of data protection law under the GDPR or the proposed legislation, without having to be mandated by an individual data subject to do so.

Key issue 17: Class actions

Dr Kelleher stated that Article 80 of the GDPR "seems to effectively provide for class actions "where provided for by Member State law"". Similarly, Dr McIntyre stated "[t]he GDPR gives us the option to effectively consolidate [data protection] cases if we allow people to nominate not-for-profit bodies to act on their behalf to bring a single action".

There is merit in considering 'class actions' in the context of the proposed legislation. In particular, it is worth considering whether 'class actions' should be explicitly provided for, or whether an enabling provision providing for same should be provided, in the proposed legislation.

3. Background

This section provides an overview of:

- the General Scheme of the Data Protection Bill (May 2017)[5] ('General Scheme');
- the legal context behind the General Scheme including the General Data Protection Regulation[6] ('GDPR') and EU Directive (EU) 2016/680[7] (also known as the 'Law Enforcement Directive' or the 'Police and Criminal Justice Authorities Directive') concerning the processing of personal data by law enforcement agencies.

3.1. General Scheme

The General Scheme was published by the Department of Justice and Equality on 12 May 2017.[8] It was referred to the Committee by the then Minister for Justice and Equality, Frances Fitzgerald, TD, on 16 May 2017.[9]

The purpose of the proposed legislation is to:

(i) give further effect to the GDPR;

(ii) transpose the Law Enforcement Directive; and

(iii) establish the Data Protection Commission (which will replace the Data Protection Commissioner) and to provide the Commission with the ability to efficiently supervise and enforce application of data protection law and standards.[10]

The proposed legislation is long and complex. The General Scheme is comprised of 96 Heads (including the Schedule) and runs to 171 pages.

Figure 1 below provides an illustrative outline of the General Scheme's 96 Heads which are divided across seven Parts in the General Scheme.

---

[5] Available at: www.justice.ie/en/JELR/General_Scheme_of_Data_Protection_Bill_(May_2017).pdf/Files/General_Scheme_of_Data_Protection_Bill_(May_2017).pdf

[6] 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. Available here: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2016_119_R_0001&from=EN

[7] 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. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG

[8] Department of Justice and Equality, Press Release: Tánaiste publishes General Scheme of Data Protection Bill 2017 (12/05/2017). Available at: http://www.justice.ie/en/JELR/Pages/PR17000155

[9] Letter from the Tánaiste and Minister for Justice and Equality to the Chairman of the Joint Committee on Justice and Equality re 'General Scheme of the Data Protection Bill 2017 Pre-Legislative Stage' dated 16 May 2017

[10] Dáil Éireann, *Written Answer No. 78 Promised Legislation*, Dáil Éireann Debates 23/05/2017 (available at: http://oireachtasdebates.oireachtas.ie/debates%20authoring/debateswebpack.nsf/takes/dail2017052300057#WRD05600 [accessed on 31/05/2017])

Figure 1: Outline of the General Scheme of the Data Protection Bill

Part 1: GENERAL PROVISIONS (Heads 1 - 5)
Part 1 deals with the short title, commencement, definitions, regulations and repeals of exisitng data protection legislation.

Part 2: DATA PROTECTION COMMISSION (Heads 6 - 15)
Part 2 contains provisions establishing Ireland's competent supervisory authority for the GDPR and the Law Enforcement Directive. It will re-establish the exisitng Data Protection Commissioner as the Data Protection Commission with one to three members.

Part 3: HEADS TO GIVER FURTHER EFFECT TO GDPR (Heads 16 - 25)
Part 3 contains provisions giving effect to discretionary provisions of the GDPR and setting down statutory procedures giving further effect to other provisions of the GDPR.

Part 4: IMPLEMENTATION OF LAW ENFORCEMENT DIRECTIVE (Heads 26 - 62)
Part 4 provides for the transposition of the Law Enforcement Directive concerning the processing of personal data by competent authorities or other entities engaged in the prevention, investigation, detection or prosecution of crime into national law. This Part is comprised of six chapters.

These are: Chapter 1 General Provisions (Heads 26-31); Chapter 2 Data subject rights (Heads 32-39); Chapter 3 Data controller and data processor obligations (Heads 40-50); Chapter 4 Transfers of personal data to third countries or international organisations (Heads 51-54); Chapter 5 Remedies, liability and penalities (Heads 55-58); and Chapter 6 Independent supervisory authority (Heads 59-62).

Part 5: EXERCISE OF SUPERVISION AND ENFORCEMENT POWERS BY DATA PROTECTION COMMISSION (Heads 63 - 89)
Part 5 contains provisions concerning the supervisions and enforcement powers of the Data Protection Commission. It also proposes "procedural safeguards" and "due process" for the exercise of those powers. This includes provisions concerning the issuing of search warrants, investigations, sanctions, offences for unauthorised disclosures or disclosure without authority of personal data and privileged legal material. This Part is comprised of five Chapters.

These are: Chapter 1 General (Heads 63-64); Chapter 2 Complaints and enforcement (Heads 65-73); Chapter 3 Investigations (Heads 74-76); Chapter 4 Sanctions (Heads 77-85); and Chapter 5 Miscellaneous (Heads 86-89).

Part 6: MISCELLANEOUS PROVISIONS (Heads 90 - 95)
Part 6 contains miscellaneous provisions. It contains provisions concerning the supervision authority for data processing operations of the courts when acting in their judicial capacity (this will not fall under the remit of the Data Protection Commission), the procedure for judicial remedies, rules of court for data protection actions, and the procedure for applications by the Data Protection Commission to refer certain cases to the Court of Justice of the European Union.

Part 7: PROVISIONS APPLICABLE TO ORAL HEARINGS CONDUCTED BY AN AUTHORISED OFFICER UNDER HEAD 67 (SCHDEULE)
Part 7 contains a Schedule setting down the procedure applying to oral hearings by authorised persons in the course of carrying out investigations under the proposed legislation.

3.2. Legal Context

The right to privacy and the right to protection of personal data are fundamental rights under EU law. This section summarises the main pieces of EU and national law regulating the processing of data.[11]

- **Irish law**

Constitution of Ireland

In Ireland, the right to privacy has been recognised by the Irish courts as an unenumerated right under Article 40.3 of the Constitution of Ireland.[12] The courts have also recognised that the right to privacy includes the right to privacy of private communications free from interference by the State, e.g. interception or surveillance.[13]

Furthermore, in *Schrems v Data Protection Commissioner*[14] the High Court stated that the accessing of private communications originating within a person's home by state authorities directly engages the Constitutional right to privacy and the right to inviolability of the dwelling under Article 40.5.

Data Protection Acts 1988 and 2003

The *Data Protection Act 1988*[15] *and the Data Protection (Amendment) Act 2003*[16] ('*Data Protection Acts*')[17] are the main pieces of legislation governing the processing of data in Ireland. The *Data Protection Acts* place legal obligations on data controllers and data processors when collecting and processing personal data such as the duty to keep personal data private and safe. In addition, the *Data Protection Acts* give people certain rights relating to their personal data.[18]

[11] For information on European Union data protection law and policy please refer to the L&RS' Note (October 2016), *European Union Data Protection Law and Policy*. Available at: http://vhlms-a01/AWData/Library2/LRSNote_EuropeaDataProtectionLawPolicy_154828.pdf
[12] *McGee v Attorney General* [1973] IESC 2; *Kennedy and Arnold v Attorney General* [1987] IR 587; *Re a Ward of Court* (No 2) [1996] 2 IR 79
[13] *Kennedy and Arnold v Attorney General* [1987] IR 587 at p. 592 and *Schrems v Data Protection Commissioner* [2014] IEHC 310 at para.47
[14] *Schrems v Data Protection Commissioner* [2014] IEHC 310 at para.48
[15] Available at: http://www.irishstatutebook.ie/eli/1988/act/25/enacted/en/html
[16] Available at: http://www.irishstatutebook.ie/eli/2003/act/6/enacted/en/html
[17] An administrative consolidated version of the Data Protection Acts (updated to 7 April 2017) is available on the Law Reform Commission website here: http://revisedacts.lawreform.ie/eli/1988/act/25/front/revised/en/html
[18] Data Protection Commissioner, *A guide to your rights* [online]. Available here: https://www.dataprotection.ie/docs/A-guide-to-your-rights-Plain-English-Version/r/858.htm

- **EU data protection law**[19]

Charter of Fundamental Rights of the European Union 2000[20]

Article 7 of the Charter of Fundamental Rights of the European Union 2000 ('EU Charter') provides for the right to respect for private and family life ('right to privacy'). Article 8 of the EU Charter formally recognised the right to protection of personal data. In doing so, the right to data protection contained therein became a specific fundamental right in EU law.[21] Under Article 51 of the Treaty on the Functioning of the European Union ('the Lisbon Treaty'), the EU institutions and Member States must observe and recognise the right to protection of personal data, including when implementing EU law.

Data Protection Directive

The 1995 Data Protection Directive (Directive 95/46/EC)[22] is the primary piece of EU law regulating the processing of personal data. The objective of the 1995 Data Protection Directive is the protection of fundamental rights and freedoms, in particular the right to privacy with respect to the processing of personal data. The Directive is transposed in Ireland through the *Data Protection Acts* and accompanying secondary regulations.

General Data Protection Regulation

The 1995 Data Protection Directive will be repealed and replaced by GDPR. The main aims of the GDPR are to harmonise data protection law across the EU Member States and to strengthen EU citizens' rights and empower them to exercise their rights.[23] The GDPR is directly applicable from the 25 May 2018. Thus, all processing of personal data must comply with the GDPR from 25 May 2018.

Although the GDPR is an EU Regulation, and EU regulations do not usually require transposition into national law (as regulations are 'directly applicable'), the GDPR contains

[19] For more information on the GDPR and the Directive (EU) 2016/680 please refer to the L&RS' Note on European Union Data Protection Law and Policy (October 2016) available here: http://vhlms-a01/AWData/Library2/LRSNote_EuropeaDataProtectionLawPolicy_154828.pdf

[20] The EU Charter may only be invoked when a domestic court is applying EU law (for more information on the EU Charter please refer to the L&RS Spotlight No.2 of 2016 *International human rights law: operation and impact*, at pp.12-13. Available at: http://data.oireachtas.ie/ie/oireachtas/libraryResearch/2016/2016-09-28_spotlight-international-human-rights-law-operation-and-impact_en.pdf [accessed on 26/05/2017])

[21] EU Agency for Fundamental Rights and Council of Europe (2014), "*Handbook on European data protection law*", at p.20. Available at: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

[22] Available here: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

[23] European Commission (n.d.), Justice Webpage '*Protection of Personal Data*'. Available at: http://ec.europa.eu/justice/data-protection/ [accessed on: 22/05/2017]

numerous provisions requiring Member State legislation. It also contains some derogations (exemptions) which Member States have the discretion of legislating for.

Article 5 of the GDPR sets down the data processing principles. Text box 1 below summarises the data processing principles.

Text box 1: Data processing principles as set out in Article 5 of the GDPR

- **Lawfulness, fairness, transparency principle** - personal data must be processed lawfully, fairly and in a transparent manner.
- **Purpose limitation principle** - personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
- **Data minimisation principle** - personal data must be adequate, relevant and limited to what is necessary.
- **Accuracy principle** - personal data must be accurate and, where necessary, kept up to date.
- **Storage limitation principle** - personal data must be kept in a form which permits identification of data subjects for no longer than is necessary.
- **Integrity and confidentiality principle** - personal data must be processed in a way that ensures appropriate security of the data.
- **Accountability principle** - the data controller must be responsible for and be able to demonstrate compliance with all the data protection principles.

In addition, the GDPR provides data subjects with a number of rights in relation to the processing of their personal data. Table 1 below briefly lists data subjects' rights under the GDPR.

Table 1: Overview of data subjects' rights under the GDPR

Right	Summary
Right to access	Article 15 provides that the data subjects have the right to access personal data concerning him or her.
Right to rectify inaccurate information	Article 16 provides that data subjects have the right to have inaccurate personal data concerning him or her rectified.
Right to erasure	Article 17 provides that data subjects have the right to have personal data concerning him or her erased in specified situations. This is also referred to as the "right to be forgotten".
Right to restriction	Article 18 provides that data subjects have the right to restrict the processing of personal data concerning him or her in specified situations.
Right to data portability	Article 20 provides that data subjects have the right to receive personal data concerning him or her in a machine readable format and to have it transmitted (transferred) to another data controller. Where technically feasible, a person can have the data transferred directly from one controller to another.
Right to object to processing	Article 21 provides a right to object to the processing of personal data where the data is processed in specified situations, including direct marketing.

Automated decisions	Article 22 provides that data subjects have the right not to be subject automated individual decision-making, including profiling.
Right to receive compensation	Article 82 provides that a person who suffers material or non-material damage due to a breach of their data protection rights has a right to receive compensation from the data controller or processor.

Law Enforcement Directive

The purpose of the Law Enforcement Directive is to establish rules for the processing of personal data by police and criminal justice authorities when being processed in connection to criminal offences and related judicial activities.[24] The Directive provides a harmonised framework under which personal data can be exchanged between Member States' police and judicial authorities. The deadline for transposition of Directive (EU) 2016/680 is 6 May 2018.

GDPR and the Law Enforcement Directive

The GDPR does not apply to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties. Such processing will be regulated by the Law Enforcement Directive.

The Directive is similar to the GDPR in that many of the data subjects' rights and data controllers and data processors obligations are similar. However, there are some modifications to those rights and obligations to take account of the fact the processing of personal data is for the purposes of law enforcement activities.[25] The General Scheme proposes that the Data Protection Commission will also be the supervisory authority for the purposes of monitoring the application of the Directive.

Some public bodies will be subject to both the GDPR and the Law Enforcement Directive depending on the processing concerned. For example, a local authority processing personal data for payroll purposes will be subject to the GDPR. However, it could be subject to the Law Enforcement Directive if it were processing personal data for the purposes of prosecuting an offence.[26]

[24] Europa (EUR-lex) (n.d.), '*Protecting personal data when being used by police and criminal justice authorities*' (from 2018). Available at: http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG [accessed on: 22/05/2017].

[25] Opening Statement of the Data Protection Commissioner, 'General Scheme of the Data Protection Bill 2017' (14/06/2017) at p.1

[26] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion'*, evidence of Seamus Carroll (official from the Department of Justice and Equality), at p.7 (14/06/2017). Available at: http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/WebAttachments.nsf/($vLookupByConstructedKey)/committees~20170614~JUJ/$File/Daily%20Book%20Unrevised.pdf [accessed on 21/08/2017]

- **Limitations to the right to privacy and right to data protection**

Neither the right to privacy nor the right to data protection are absolute rights. The Lisbon Treaty recognises that the right to data protection must be balanced against other rights and freedoms.[27] In addition to the obligation to set down data protection rules, Article 16 of the Lisbon Treaty provides that EU legislators must also set down rules for the free movement of personal data.

The EU Charter also provides that the rights contained in it may be limited, where the limitation is set down in law and it respects the 'essence' of the right being limited. Under Article 52 of the EU Charter, any limitations must be limited to what is proportionate and necessary, and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

In Ireland, the High Court in *Schrems v Data Protection Commissioner* recognised that the interception of private communications by the State is not in itself necessarily unlawful. The Court stated that where appropriate safeguards are in place, the interception or electronic surveillance of communications may be lawful where it is indispensable for the preservation of State security.[28]

- **Children's rights**

The GDPR contains a number of provisions concerning children. Article 8 of the GDPR requires that consent for children below 16 years of age to use information society services must be given or authorised by the holder of parental responsibility. Member States may lower the digital age of consent to 13 years.

Other provisions regarding children in the GDPR include:

- **Article 6(1)(f)** provides for the processing of personal data where it is necessary for the purposes of legitimate interest, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (emphasis added).
- **Article 8(2)** requires data controllers to "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" (emphasis added). Under Article 83, a breach of this provision could result in a fine of up to €10 million or up to 2% of the total worldwide annual turnover for the previous year (whichever is higher).

[27] Karen Murray (2016), '*EU Data Protection Reform*', (2016) 34 Irish Law Times 26-28
[28] *Schrems v Data Protection Commissioner* [2014] IEHC 310 at para.49

- **Article 12** relates to transparency of information and communication that is given to data subjects to enable them to exercise their rights. It requires data controllers to take appropriate measures to provide any communication and information in a "concise, transparent, intelligible and easily accessible form, using clear and plain language" for data subjects, especially children.
- **Article 40** encourages the drawing up of various codes of conduct by associations and other bodies representing categories of data controllers or processors to help ensure the GDPR is properly applied. Codes of conduct which may be drawn up include ones concerning "the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained".
- **Article 57** provides that, when carrying out its promotion of public awareness tasks under the GDPR, the national supervisory authority must pay special attention to activities addressed to children.
- **Recital (38)**[29] provides that:

  > "[c]hildren merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."

- **Recital (58)**[30] discussing the requirement to provide information that is accessible and easy to understand when addressing the public provides "[g]iven that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."
- **Recital (65)**[31] concerning the right to be forgotten provides that this right "is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet".
- **Recital (71)**[32] concerning the right not to be subject to automated individual decision-making, including profiling, provides that the derogations restricting this right in the GDPR "should not concern a child".
- **Recital (75)**[33] provides that the risk to the rights and freedoms of natural persons that may result from the processing of their personal data which could lead to physical, material or non-material damage, in particular includes, among other things "personal data of vulnerable natural persons, in particular of children."

[29] **Note**: Recitals do not have the status of law. However, they do provide guidance of the intent of the law and should be taken as a strong indication of how the law should be interpreted and implemented.
[30] *ibid.*
[31] *ibid.*
[32] *ibid.*
[33] *ibid.*

United Nations Convention on the Rights of the Child

The United Nations Convention on the Rights of the Child[34] ('UNCRC') is relevant to the consideration of children in the context of the GDPR. For example, as noted in the Department of Justice and Equality consultation on the digital age of consent:

> "Article 5 of the UN Convention on the Rights of the Child recognises the right and duty of parents and guardians to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by children of their rights."

Article 12 of the UNCRC provides that "children who are capable of forming their own views enjoy the right to express these views freely in matters affecting them and that due weight be given to them".[35]

Other children's rights under the UNCRC relevant to the on-line environment include:[36]

- **Article 2** concerning children's right to non-discrimination;
- **Article 3** concerning children's right to have their best interest treated as the primary interest in all matters affecting him/her;
- **Article 5** concerning children's evolving capacities;
- **Article 13** guaranteeing children's enjoyment to the right of freedom of expression, including the right to seek, receive and impart information and ideas;
- **Article 14** concerning children's right to freedom of thought, conscience and religion;
- **Article 15** concerning children's right to freedom of association and assembly;
- **Article 16** concerning children's right to protection from arbitrary and unlawful interference with privacy, family, home or correspondence; and
- **Article 17** concerning the right to freedom of information, including the right to access information from a variety of sources and to be protected from harmful information;

---

[34] Available at: http://www.ohchr.org/Documents/ProfessionalInterest/crc.pdf

[35] Cited in the Department of Justice, *Data protection safeguards for children ('digital age of consent') Consultation paper* (November 2016). Available at: http://www.justice.ie/en/JELR/Pages/Consultation_paper_Data_protection_safeguards_for_children_(%E2%80%98digital_age_of_consent%E2%80%99)

[36] Ombudsman for Children, '*Preliminary Observations of the Ombudsman for Children's Office on the General Scheme of the Data Protection Bill 2017 Submission to the Oireachtas Joint Committee on Justice and Equality*' (29/06/2017) at p.2 and Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Dr Geoffrey Shannon (Special Rapporteur on Child Protection), at pp.20-21 (05/07/2017). Available at: http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/WebAttachments.nsf/(SvLookupByConstructedKey)/committees~20170705~JUJ/$File/Daily%20Book%20Unrevised.pdf [accessed on 21/08/2017]

- **Articles 19, 34** and **36** concerning children's right to be protected from all forms of violence, abuse and exploitation;
- **Article 24** concerning children's right to the highest attainable standard of health;
- **Articles 28** and **29** concerning children's right to education;
- **Article 31** concerning children's right to engage in play and recreational activities and to participate freely in cultural life and the arts.

4. Structure of data protection law

This section sets out stakeholders' recommendations during PLS on the General Scheme concerning the repeal of existing data protection law and the structure of the proposed Data Protection Bill.

3.1. Repeal of existing data protection legislation

- **General Scheme**

Head 5 of the General Scheme, entitled "*Repeals*", is blank. The Explanatory Notes to Head 5 state that the *Data Protection Act 1988*[37] *and the Data Protection (Amendment) Act 2003*[38] ('*Data Protection Acts*') "will largely be superseded by provisions in the GDPR and Part 4 of this Bill which give effect in national law to the law enforcement Directive".[39]

It is not clear from Head 5 of the General Scheme if the *Data Protection Acts* will be partially repealed or repealed in their entirety. During PLS hearings, stakeholders recommended the repeal of the *Data Protection Acts* in their entirety.

- **Evidence to the Committee**

Mr Seamus Carroll (official from the Department of Justice and Equality) in evidence stated the matter of repealing the *Data Protection Acts* "is still under consideration".[40] He explained that the GDPR does not apply to processing of personal data in the course of an activity which falls outside the scope of EU law, such as national security.[41]

The Data Protection Commissioner ('Commissioner') in her written statement disagreed with retaining any parts of the *Data Protection Acts*. The Commissioner stated that, as she understood it, the parts of the *Data Protection Acts* that might not be repealed relate to the *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*[42] ('Convention 108'). She explained that "[t]he concern, therefore, is that, if our existing Data Protection Acts are repealed, some elements of Convention 108

[37] Available at: http://www.irishstatutebook.ie/eli/1988/act/25/enacted/en/html
[38] Available at: http://www.irishstatutebook.ie/eli/2003/act/6/enacted/en/html
[39] An administrative consolidated version of the Data Protection Acts (updated to 7 April 2017) is available on the Law Reform Commission website here: http://revisedacts.lawreform.ie/eli/1988/act/25/front/revised/en/html
[40] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion'*, evidence of Seamus Carroll, at p.3 (14/06/2017)
[41] Ibid.
[42] Available at: https://rm.coe.int/1680078b37

may also fall away, putting Ireland in breach of its commitment to implement the convention in full".[43]

The Commissioner went on to say, in evidence, that:[44]

> "[t]he Irish DPC is of the view that if the pieces of the 1988 and 2003 Acts [are] to be retained [and] are capable of identification, it must be possible to fully repeal those Acts and rewrite the small number of provisions that require retention into a new stand-alone Bill."

In her written statement, the Commissioner outlined a number of reasons why the *Data Protection Acts* should be repealed in their entirety. Those reasons fall under the following headings:

(i) accessibility and legal certainty;

(ii) a new era in data protection law and reputational consequences; and

(iii) Ireland as a lead supervisory authority.

The Commissioner's evidence relating to these are summarised below.

(i) Accessibility and legal certainty

The Commissioner stated that as the Data Protection Bill can only provide for supplementary provisions to the GDPR. As a result, individuals will need to read both the GDPR and the Data Protection Bill when looking at data protection law. Retaining parts of the *Data Protection Acts* will result in individuals having "to weave their way through a dense legislative maze of three separate legislative sources" i.e. individuals will have to read the GDPR, the *Data Protection Acts* and the Data Protection Bill when trying to understand their data protection rights and obligations.[45]

The effect of which, the Commissioner stated could result in decreased levels of compliance. In this context the Commissioner stated:[46]

> "[t]he DPC strongly holds the view that the more complicated a piece of legislation is, the less likely it is to be fully understood by the stakeholders to whom it is addressed, resulting in diminished compliance levels. For this reason, and given the greatly enhanced obligations on data controllers and processors under the GDPR, it is critical

[43] Opening Statement of the Data Protection Commissioner, 'General Scheme of the Data Protection Bill 2017' (14/06/2017) at pp.6-7
[44] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion'*, evidence of Helen Dixon (Data Protection Commissioner), at p.19 (14/06/2017). Available at: http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/WebAttachments.nsf/($vLookupByConstructedKey)/committees~20170614~JUJ/$File/Daily%20Book%20Unrevised.pdf [accessed on 21/08/2017]
[45] Opening Statement of the Data Protection Commissioner, 'General Scheme of the Data Protection Bill 2017' (14/06/2017) at p.6
[46] Ibid., at p.5

that the GDPR is given effect in the State by way of legislation that is clear, certain and free from ambiguities."

The Commissioner went on to say that:[47]

> "[t]he DPC does not believe that this will be achieved by retaining parts of the existing legislation and over-layering them with new legislative provisions in the Data Protection Bill, as this will cause confusion and interpretative difficulties."

(ii) A new era in data protection law and reputational consequences

The Commissioner, in her written statement, observed that retaining portions of existing data protection law "is not consistent with the EU policy objective of a new modernised data protection regime heralded by the GDPR" which aims to harmonise data protection law across the EU. She went on to say that:[48]

> "[a] patchwork legislative framework consisting of statutory provisions which are in the case of the 1988 Data Protection Act) 29 years old, combined with updated statutory provisions (designed to take account of the digital revolution) could be perceived as a lack of commitment to the new data protection regime in the EU and could be damaging for the State's and the DPC's reputation."

(iii) Ireland as a lead supervisory authority

Under the GDPR, the DPC will become the "lead supervisory authority" for multinational companies who have their European headquarters in Ireland. The Commissioner in her written statement stated that she believes that existing international interest in the DPC will increase once the GDPR comes into force. She stated that:[49]

> "[t]here will inevitably be a huge amount of scrutiny as to the domestic measures taken by the State to give effect to the GDPR. This makes it all the more critical that Ireland's domestic legislative framework is as simple and accessible as possible so that Ireland is perceived as having, and actually has, a robust but accessible legislative framework which is appropriate to the critical role which the DPC will perform as a lead supervisory authority under GDPR."

The Commissioner went on to say that retaining portions of existing data protection law will undermine the aim of the Government's message that "Ireland will be 'best in class', leading the way in best practice in European data protection regulation".[50]

In evidence the Commissioner summed up reasons for not retaining any parts of the *Data Protection Acts* in the following:[51]

[47] Ibid., at p.5
[48] Ibid., at p.6
[49] Ibid.
[50] Ibid.

> "the GDPR is intended to represent a clean slate, establishing a single legal instrument in which data protection rules and principles will be set out …
>
> We consider that their retention runs the risk of creating legal uncertainty in terms of precisely which provisions of the law will apply and in what circumstances post-May 2018, let alone considering how inaccessible for those seeking to comply with the law such an arrangement would be. In addition, a patchwork presentation of the new Irish law in the form of a 2018 amendment Act rather than a completely new stand-alone Act does not create the impression of a new, modernised regime.
>
> Further, given the Irish DPC's obligations under the GDPR to co-operate in law with other European data protection authorities, a patchwork presentation would undermine confidence in Ireland's ability to regulate the multinationals located here."

Dr TJ McIntyre (representative from Digital Rights Ireland ('DRI')), in evidence agreed, that "the residual parts of the 1988 and 2003 Acts should be repealed and re-enacted as a stand-alone instrument rather than being left in place".[52] Dr McIntyre stated that:[53]

> "[i]t seems that if we leave any Parts of the 1988 and 2003 Acts in place, we will have a position where to deal with certain matters, in particular those with an overlap between public and private processing of data, we will have to look to the 1988 Act, determine how it was amended by the 2003 Act, determine how that was amended by what would be the 2018 Act and then look to the GDPR on top of that, possibly while looking to other European instruments on top of that as well. For example, these might include European instruments regarding the Schengen information system. It seems that would be a real recipe for confusion."

Dr McIntyre also stated that the parts of the *Data Protection Acts* being retained relate to the Convention 108. He went on to say:[54]

> "[t]he Council of Europe [C]onvention on the [P]rotection of [P]ersonal [D]ata is in the process of being modernised and we are at a point where we are very close to agreement on a final text. This is something that will be implemented certainly in the next couple of years in any event. It would be very useful at this point to pre-empt that as far as possible by separating those provisions."

Dr Denis Kelleher (Barrister-at-Law) in evidence agreed with the DPC that a "patchwork presentation" of Ireland's data protection law does not "create the impression of a new, modernised regime".[55] However, he went on to express concerns for reasons of timeliness with the feasibility of repealing the *Data Protection Acts* in their entirety. He explained that:[56]

---

[51] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion'*, evidence of Helen Dixon, at pp.18-19 (14/06/2017).
[52] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Dr TJ McIntyre (representative of Digital Rights Ireland), at p.2 (05/07/2017). Available at: http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/WebAttachments.nsf/($vLookupByConstructedKey)/committees~20170705~JUJ/$File/Daily%20Book%20Unrevised.pdf [accessed on 21/08/2017]
[53] Ibid., at pp.2-3
[54] Ibid., at p.3
[55] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Dr Denis Kelleher (Barrister-at-Law), at p.3 (21/06/2017). Available at:

> "[t]he Data Protection Bill has to be on the Statute Book by May next year. … If we were to try to do these two things at the same time, namely, set out the residual regime which potentially is still significant and the new GDPR regime, I question whether the Oireachtas would be able to allocate the proper length of time to debate the legislation."

Dr Kelleher queried whether the Parliamentary Counsel could address the issue as part of the drafting of the proposed legislation. For example, he wondered if we could have an entirely new Data Protection Bill while leaving behind a separate and distinct "rump regime" that could be dealt with at a later stage.[57]

Recommendation 1: Repeal of the *Data Protection Acts*

The Committee recommends that the old *Data Protection Acts* should be repealed in their entirety. Provisions within these Acts which may require retention can be preserved by enacting standalone legislation.

3.2. Structure of the proposed Data Protection Bill

As is evidenced by the length and complexity of this General Scheme, data protection law is a complex and nuanced area. During the PLS hearings, stakeholders recommended that the Law Enforcement Directive is transposed in a separate piece of legislation. It was also recommended that the GDPR should be annexed or appended to the proposed legislation in order to make the proposed legislation more accessible.

- **Evidence to the Committee**

Dr McIntyre, in evidence, said that Part 4 of the General Scheme transposing the Law Enforcement Directive should be provided for in a separate piece of legislation. He stated that the current structure of the General Scheme has resulted in confusion. He gave the example of people reading Part 4 of the General Scheme transposing the Law Enforcement Directive but thinking it related to the GDPR.[58]

Mr Simon McGarr (representative of DRI) noted that the General Scheme aims to do three things: give further effect to the GDPR; transpose the Law Enforcement Directive; and replace the *Data Protection Acts*. Mr McGarr stated that:[59]

---

http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/WebAttachments.nsf/($vLookupByConstructedKey)/committees~20170621~JUJ/$File/Daily%20Book%20Unrevised.pdf [accessed on: 21/08/2017]

[56] Ibid., at pp.3-4

[57] Ibid., at p.4

[58] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Dr TJ McIntyre, at p.2 (05/07/2017)

[59] Ibid., at p.7

> "[w]e do not think it is a good idea to attempt to do those three things because this legislation must be passed and it is on a deadline. The GDPR comes into force in May of next year and by running the implementation measures in respect of the GDPR together with the complicated matters in transposing a directive and the partial repeal of the data protection Acts, we run the risk from a practical point of view of either legislative gridlock preventing the matter from progressing at the required speed, or of the matter passing without the necessary scrutiny in respect of one area of the Bill because there is such a pressing deadline in respect of other areas."

Mr McGarr went on to say DRI recommend that the Law Enforcement Directive is transposed in a separate legislative instrument. He stated:[60]

> "[DRI] recommend that it is better to address the transposition of Directive 216/680 by way of a specific legislative instrument separately. This would allow any of the necessary residual elements required from the [D]ata [P]rotection Acts for that transposition, or as a result of the requirements of the State as a member of the Council of Europe, to be dealt with separately in another issue. This would then allow for the full repeal of the existing [D]ata [P]rotection Acts which are intended for partial repeal under [H]ead 5 and their replacement by the GDPR in Irish law."

Recommendation 2: Legislate separately for the Law Enforcement Directive

The Committee recommends that the Law Enforcement Directive be transposed in separate legislation to the General Scheme addressed in this report.

Dr McIntyre also stated that DRI "think it would be a good idea if the GDPR is reproduced as either an annexe or appendix verbatim in the final Bill, together with a few domestic legislative variations which are provided for under the regulation".[61] Benefits of this highlighted by Dr McIntyre include:[62]

> "[a]s well as providing clarity for users and the courts in the consideration of what is quite a complex area of law … It also significantly reduces the chance of any legislative uncertainty as to what provisions are being applied by the court at any given moment. Therefore, the likelihood of challenges to the interpretation by the new Data Protection Commission before the courts is reduced."

Dr McIntyre went on to say:[63]

> "[t]hat is a valuable aim in itself. The Data Protection Commission, which is set up, will be a new body exercising significant new powers and it is important for building up confidence in that body, but also in respect of the courts relationship with that body as a place of appeal from its decision making, that exactly the laws it is working under and exactly the powers it is implementing are as clearly set out by the Oireachtas, in advance of the commencement of the commission in order to allow the commission to fully

[60] Ibid.
[61] Ibid., at p.7
[62] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Simon McGarr (representative of Digital Rights Ireland), at p.7 (05/07/2017). Available at: http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/WebAttachments.nsf/($vLookupByConstructedKey)/committees~20170705~JUJ/$File/Daily%20Book%20Unrevised.pdf [accessed on 21/08/2017]
[63] Ibid.

exercise its rights without the fear of constant challenge, which we have seen in previous regulatory systems which have been introduced. Particularly where large amounts of financial administrative fines are at stake there is an incentive for judicial challenge."

Recommendation 3: Include the GDPR text within the new legislation

The Committee recommends that the text of the GDPR be included verbatim in the proposed legislation as an appendix. This will help ensure transparency and consistency when the legislation is enacted.

In addition, Dr McIntyre stated that after the completion of the legislative process it would be helpful if a consolidated document was produced and published by either the Department of Justice and Equality or the DPC that included the text of the GDPR and the corresponding provisions of national law.[64]

Recommendation 4: Structure of the proposed legislation

Following the enactment of the proposed legislation, consideration should be given to producing an administrative consolidated version of the GDPR with the corresponding national law provisions. This will result in individuals only having to read through one document when ascertaining their data protection rights and obligations. This would make data protection law more accessible and aid the safeguarding of citizens' fundamental right to protection of their personal data.

[64] Ibid., at p.17

5. Children's rights

The GDPR sets down numerous of obligations with regard to the processing of children's personal data. Stakeholders made a number of recommendations in respect of the General Scheme from a children's rights perspective during PLS.

- **General Data Protection Regulation**

Regarding the 'digital age of consent' (the age at which a child can consent to use online services), Article 8(1) of the GDPR requires consent for children below 16 years of age to use information society services is given or authorised by 'the holder of parental responsibility'. Member States may lower the age of digital consent to 13 years.[65]

Article 8(2) of the GDPR requires data controllers to "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". Under Article 83 of the GDPR, a breach of this provision could result in a fine of up to €10,000,000 or up to 2% of the total worldwide annual turnover for the previous year (whichever is higher).

Article 9(2) of the GDPR provides that Member States may, by law, derogate from the prohibition on processing sensitive personal data such as data revealing racial or ethnic origin in specified instances e.g. where it is necessary for reasons of substantial public interest.

- **General Scheme**

Head 16 of the General Scheme, entitled "*Child's consent in relation to information society services [Article 8]*", proposes to set the digital age of consent for Ireland. Head 16 is blank as to the digital age of consent.[66] The Irish Times reported that on 26 July 2017, the Cabinet agreed that the digital age of consent should be set at 13 years of age.[67]

Head 17 of the General Scheme, entitled "*Processing of special categories of personal data for reasons of substantial public interest [Article 9.2(g)*", proposes to grant the Minister discretionary power, by Regulations, to permit the processing of special categories of personal

[65] The original proposal for the GDPR proposed 13 years of age as the minimum as the digital age of consent. However, this was raised to 16 years of age in during the European Parliaments final negotiations.

[66] In November 2016, the Department of Justice launched a public consultation on "*Data protection safeguards for children ('digital age of consent')*"[66] on what the statutory digital age of consent should be for children to use information society services offered directly to them, as required under the GDPR. Available at : http://www.justice.ie/en/JELR/Consultation_paper_Digital_Age_of_Consent.pdf/Files/Consultation_paper_Digital_Age_of_Consent.pdf [accessed on 06/09/2017]

[67] Mary Minihan, '*Cabinet agrees to set 'digital age of consent' at 13*', The Irish Times (26/07/2017). Available at: http://www.irishtimes.com/news/social-affairs/cabinet-agrees-to-set-digital-age-of-consent-at-13-1.3167987 [accessed on 25/08/2017]

data for reasons of "substantial public interest". Such Regulations are to "respect the essence" of the right to data protection and contain "suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject".

Head 18 of the General Scheme, entitled "*Processing of special categories of personal data [Article 9.2 (b), (h), (i) and (j) and 4]*", proposes that the categories of sensitive data listed in Head 18(1) may be processed where necessary for, among other things, "the management of health and social care systems and services and for public interest reasons in the area of public health." The processing of such data are to be "[s]ubject to suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject".

The Explanatory Notes to Head 18 state that:

> "[t]here 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."

- **Evidence to the Committee**

Dr Shannon's evidence focussed specifically on children's rights issues. He stated that from a children's rights perspective, certain aspects of the General Scheme required particular attention. His evidence focussed on the following issues:

(i) the digital age of consent;
(ii) the need for certain definitions relating to children and data protection;
(iii) the right to be forgotten;
(iv) the link between data protection and digital safety; and
(v) the processing of sensitive personal data.

In the context of discussing the digital age of consent, Dr Shannon also emphasised the right of children to participate in matters affecting them and recommended carrying out consultations with children on the proposed legislation.

Evidence relating to the issues highlighted above is summarised below. This section of the Paper will also summarise evidence from Dr Kelleher regarding the legal obligation in the GDPR to process personal data for the purposes of identifying persons ('identification services') e.g. to distinguish between adults and children on-line.

5.1. Digital age of consent

Evidence from a number of children's rights organisations, and their advocates, to the Committee were in agreement that the digital age of consent should be set at 13 years of age.

- **Evidence to the Committee**

For example, **Dr Shannon** stated that setting the digital age of consent at 13 years of age would help to ensure that children can practically enforce their rights such as, the right to participate in matters concerning him/her, right to be heard, right to express themselves freely and the right to access information need to be exercised effectively by children.[68]

Dr Shannon also stated the **Children's Rights Alliance** (of which Dr Shannon is the founding patron) agreed that the digital age of consent should be set at the lower age of 13.[69]

The **Ombudsman for Children**, in his written submission, also stated the digital age of consent should be set at 13 years of age.[70]

Other commentary on the digital age of consent

Dr Mary Aiken (cyber-psychologist) and **Mr O'Sullivan** (Professor, Department of Computer Science, University College Cork), responding in The Irish Times to the recommendation the digital age of consent should be set at 13 years of age, noted that in a psychological context children mature at different rates.[71] They stated that Ireland:[72]

> "should arguably legislate towards the upper end of the relevant age band – perhaps closer to 16 than 13 – in order to protect the children who are less well equipped to deal with the complexities that digital consent presents."

Recommendation 5: Digital age of consent

The Committee recommends that the digital age of consent be set at 13 years of age. The Committee also recommends that this age of consent be reviewed at appropriate intervals to ensure it remains suitable as technology evolves.

[68] Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Dr Geoffrey Shannon, at p.21 (05/07/2017)
[69] Ibid.
[70] Ombudsman for Children, '*Preliminary Observations of the Ombudsman for Children's Office on the General Scheme of the Data Protection Bill 2017 Submission to the Oireachtas Joint Committee on Justice and Equality*' (29/06/2017) at p.8
[71] Mary Aiken, Barry O'Sullivan, '*We need to talk about the Irish 'digital age of consent*", The Irish Times (13/07/2017). Available at: https://www.irishtimes.com/opinion/we-need-to-talk-about-the-irish-digital-age-of-consent-1.3152388 [accessed on 25/08/2017]
[72] Ibid.

Consultation with children

Referring to Article 12 of the UNCRC concerning the right of children to express their opinion, Article 24 of the EU Charter concerning the rights of the child and the 2012 Children Referendum, **Dr Shannon** highlighted the importance of the 'voice of the child' and 'children's right to participate in all matters' concerning him or her.[73] He also referred to the 'National Strategy on Children and Young People's Participation in Decision-Making 2015-2020',[74] the goal of which he said:[75]

> "is to ensure that children and young people have a voice in their individual and collective everyday lives and it explicitly acknowledges that their voice in decision-making requires a cross-Government response, with initiatives and actions from all key Departments and agencies."

Dr Shannon stated that it is unclear whether children have been consulted on the proposed digital age of consent. Noting the "integral role" information services technology and digital media play in the lives of young people, Dr Shannon recommended that "a consultation process takes place to ascertain the views of a variety of age groups of children on the issue of digital consent". He stated that at the very least a focus group should be carried out.[76] As to how such consultation could be realised, he stated that a request could be made of the Ombudsman for Children to assist or that the Children's Rights Alliance has conducted similar exercises.[77]

The **Ombudsman for Children** also stated that children should be given the opportunity to express their views, and have those views taken into account, on parts of the proposed legislation that affect children.[78]

Recommendation 6: Consultation with children

The Committee recommends that a detailed consultation take place with children of all ages to ascertain their views on the proposed measures for data protection.

[73] Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Dr Geoffrey Shannon, at p.20 (05/07/2017)
[74] Department of Children and Youth Affairs (2015), 'National Strategy on Children and Young People's Participation in Decision-making, 2015 – 2020.' Dublin: Government Publications. Available at: www.dcya.ie at https://www.dcya.gov.ie/documents/playandrec/20150617NatStratonChildrenandYoungPeoplesParticipationinDecisionMaking2015-2020.pdf
[75] Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Dr Geoffrey Shannon, at p.20 (05/07/2017)
[76] Ibid.
[77] Ibid., at p.27
[78] Ombudsman for Children, '*Preliminary Observations of the Ombudsman for Children's Office on the General Scheme of the Data Protection Bill 2017 Submission to the Oireachtas Joint Committee on Justice and Equality*' (29/06/2017) at p.3

5.2. Definitions relating to children and data protection

Neither the GDPR nor the General Scheme defines 'children' or the 'child'. The **Ombudsman for Children** recommended the proposed legislation provide a definition of 'child'. The Ombudsman stated:[79]

> "[t]he Data Protection Bill 2017, once drafted, should include an explicit definition of the 'child' and this definition should be in keeping with the UNCRC's [Article 1] definition of the 'child' as every human being below the age of eighteen years."

Recommendation 7: Definition of 'child'

The Committee recommends that a definition of who is a 'child' be included in the proposed legislation. The definition of 'child' – as per Article 1 of the UNCRC – should include every human being below 18 years of age.

Head 16 of the General Scheme concerning the digital age of consent proposes to provide that consent is required from 'the holder of parental responsibility' for children below the digital age of consent. The General Scheme does not define 'the holder of parental responsibility'.

Dr Shannon, in evidence, stated the term "[p]arental responsibility" is more common to the United Kingdom and is not defined in Irish law.[80] In his written statement, he explained the term 'the holder of parental responsibility' is taken directly from the GDPR and "has no clear meaning under Ireland's existing statutes concerning children".

Dr Shannon recommended that the term should be clarified so that those it applies to are clearly identifiable.[81] Noting the enhanced rights for a large number of citizens with respect to children and families under the *Children and Family Relationships Act 2015,*[82] he stated the term should be broadly defined to "include any parent and guardian of the child, whether automatic or court appointed pursuant to the Guardianship of Infants Act 1964."[83]

Recommendation 8: Definition of 'the holder of responsibility'

The term 'holder of parental responsibility' in Head 16 is not defined within the proposed legislation, and the Committee recommends that a broad definition of parental responsibility be applied, to include natural or court-appointed responsibility.

---

[79] Ombudsman for Children, '*Preliminary Observations of the Ombudsman for Children's Office on the General Scheme of the Data Protection Bill 2017 Submission to the Oireachtas Joint Committee on Justice and Equality*', at p.6 (29/06/2017)
[80] Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Dr Geoffrey Shannon, at p.22 (05/07/2017)
[81] Dr Geoffrey Shannon (n.d.), '*Joint Committee on Justice and Equality Submission Dr Geoffrey Shannon, Special Rapporteur on Child Protection*' at p.6
[82] Available at: http://www.irishstatutebook.ie/eli/2015/act/9/enacted/en/html
[83] Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Dr Geoffrey Shannon, at p.22 (05/07/2017)

Dr Shannon, in his written submission, noted that Recital (38) of the GDPR provides that "the consent of the holder of parental responsibility for the child should not be necessary in the context of "preventative or counselling services offered directly to a child"".[84] Neither the GDPR nor the General Scheme defines 'preventative or counselling services'.

In evidence, Dr Shannon stated that it is not clear whether the range of preventive or counselling services offered to children will fall within the scope of 'preventive or counselling services' and recommended it be defined. He stated:[85]

> "whether the variety of service providers envisaged in that context will come within the definition of "preventive or counselling services" is unclear and needs to be clarified. For this reason, I am suggesting that consideration be given to defining "preventive or counselling services" in the broadest possible fashion so that children can avail of support when they need it."

Recommendation 9: Definition of the 'preventive or counselling services'

The Committee recommends that a broad range of defined preventative and counselling services be provided to children to enable them to deal with data protection issues when they so need.

5.3. The right to be forgotten and children

Dr Shannon emphasised the importance of the right to be forgotten (referred to as 'the right to erasure' in the GDPR) in the context of children. He stated that:[86]

> "[i]t is probably even more important for children, as they are less likely than adults to be aware that information they post online may be available long term. They may not consider the consequences of posting something online which may last long beyond their childhood."

He said that there is no provision in the General Scheme giving effect to the right to be forgotten as provided for in Article 17 of the GDPR.[87]

Dr Shannon suggested that "Ireland should take the opportunity to include specific provisions on this issue" in the proposed legislation. He also stated that alongside the right to be

[84] Dr Geoffrey Shannon (n.d.), '*Joint Committee on Justice and Equality Submission Dr Geoffrey Shannon, Special Rapporteur on Child Protection'* at p.6
[85] Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Dr Geoffrey Shannon, at pp.21-22 (05/07/2017)
[86] Ibid., at p.23
[87] Head 35 of the General Scheme concerns the right to rectification, erasure or restriction of processing for the purposes of the Law Enforcement Directive only.

forgotten "there must be a procedure for taking down in a timely fashion offensive material posted online".[88]

Regarding the latter point about the 'take-down' procedure, it is noteworthy that since the Court of Justice of the European Union (CJEU) ruled that there is a right to be forgotten decisions whether to de-list search results as a result of the right to be forgotten being successfully invoked are made and decided upon by search engine operators.[89] Some privacy experts have expressed concern over the lack of transparency of the procedure used by search engine operators in handling such requests.[90]

The **Ombudsman for Children** stated that it is not clear from the GDPR if children can exercise a right to be forgotten or whether the exercise of the right is confined to adults. The Ombudsman, referring to the right to rectification and the right to erasure, stated the proposed legislation should explicitly reference children. He stated:[91]

> "[w]e believe that children and young people should be able to exercise the right to erasure of their personal data when they are still children and young people, subject to lawful restrictions. Allowing for children and young people to do so would be a protective measure that would take account, among other things, of Recital 38 of the GDPR, which acknowledges that "children merit specific protection with regard to their personal data, as they may be less aware of the risk, consequences and safeguards concerned … in relation to the processing of their personal data." Accordingly, we are of the view that provisions in the Bill concerning the right to rectification and erasure should make explicit reference to children and young people's right in this regard."

Recommendation 10: Right to be forgotten and children

Owing to their particular vulnerability online, the Committee recommends that children be granted a specific and explicit right to be forgotten online.

5.4. The link between data protection and digital safety

Stakeholders during PLS highlighted the importance of the link between data protection and digital safety.

[88] Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Dr Geoffrey Shannon, at pp.23 & 24 (05/07/2017)
[89] Library & Research Service Note on '*European Union Data Protection Law and Policy*', at pp.10-11 (27/10/2016). Available at: http://vhlms-a01/AWData/Library2/LRSNote_EuropeaDataProtectionLawPolicy_154828.pdf [accessed on 25/08/2017]
[90] Ibid.
[91] Ombudsman for Children, '*Preliminary Observations of the Ombudsman for Children's Office on the General Scheme of the Data Protection Bill 2017 Submission to the Oireachtas Joint Committee on Justice and Equality*' (29/06/2017) at p.12

- **Evidence to the Committee**

Dr Shannon said:[92]

> "[d]igital safety is not about creating a nanny state; it is about empowering young people to understand the benefits and downsides of the online world, especially in terms of young people's exposure to cyberbullying. There is another important and profound question in respect of adult data literacy. Much more needs to be done in this jurisdiction."

The **Ombudsman for Children** recommended that appropriate measures are taken "to develop and strengthen the digital literacy competencies and skills of children, young people and parents/guardians".[93]

Dr Mary Aiken and **Mr O'Sullivan**, commenting in The Irish Times on evidence from stakeholders during PLS hearings on the General Scheme, stated that:[94]

> "Ireland also needs to put in place a policy framework and an associated educational programme that ensures that our children are sufficiently aware and responsible to understand and exercise their digital rights by the time they reach the digital age of consent."

Recommendation 11: Policy framework and educational programme to assist children in exercising their digital rights before they reach the digital age of consent

The Committee recommends that a policy framework and an associated educational programme be implemented to assist children in exercising their digital rights before they reach the digital age of consent.

5.5. Processing sensitive personal data of children

Stakeholders stated during PLS that it is inevitable that Tusla - the Child and Family Agency (CFA) will process sensitive personal data of children and young people and that additional safeguards should be provided where such sensitive personal data is being processed.

- **Evidence to the Committee**

Dr Shannon, in his written statement, stated it is conceivable Head 18 of the General Scheme concerning the processing of sensitive personal data for the purposes of "the management of health and social care systems and services and for public interest reasons in the area of public

[92] Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Dr Geoffrey Shannon, at p.18 (05/07/2017)
[93] Ombudsman for Children, '*Preliminary Observations of the Ombudsman for Children's Office on the General Scheme of the Data Protection Bill 2017 Submission to the Oireachtas Joint Committee on Justice and Equality*' (29/06/2017) at p.8
[94] Ibid.

health" will enable the CFA to process such data. In evidence he said that this will "inevitably include [processing] special sensitive data relating to children and young persons".[95]

Regarding whether the safeguards required for such processing are to be additional or complementary to data controller obligations in the GDPR, Dr Shannon recommended they should be in addition. He submitted that:[96]

> "[g]iven the nature of the data involved, it is recommended that consideration be given to the inclusion of additional safeguards, particularly where a child's sensitive personal data is engaged and is to be processed by the CFA. This should be explored having regard to Recital 38 of the GDPR and the special protection required therein for the personal data of children."

Recommendation 12: Additional safeguards for the processing of sensitive personal data

The Committee recommends that additional safeguards be implemented to ensure that the processing of a child's sensitive data under Head 18 is conducted in a safe manner.

5.6. Provision of identification services

Stakeholders gave evidence during PLS that under the GDPR there is a legal obligation to process personal data for the purposes of identifying persons ('identification services') and consideration should be given to who provides such services.

- **Evidence to the Committee**

Dr Kelleher In evidence stated that under the GDPR there is a legal obligation to carry out identification services. He explained that:[97]

> "[s]ocial media providers and persons engaged in profiling will have to be able to distinguish between children and adults. That is a legal obligation. They are subject to onerous fines and open potentially to very serious claims for damages if they process the data of children where they are not supposed to do so. Social media providers, fintech firms and so on will have to be able to identify who is and is not a child."

Dr Kelleher questioned who is going to provide identification services. He stated there are two choices; either the State will provide identification services or private bodies will.[98] Dr Kelleher went on to say that it would be better if the State provided such services. He said that:[99]

---

[95] Dr Geoffrey Shannon (n.d.), '*Joint Committee on Justice and Equality Submission Dr Geoffrey Shannon, Special Rapporteur on Child Protection'* at p.9
[96] Ibid., at p.10
[97] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Dr Denis Kelleher (Barrister-at-Law), at p.4 (21/06/2017). Available at: http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/WebAttachments.nsf/($vLookupByConstructedKey)/committees~20170621~JUJ/$File/Daily%20Book%20Unrevised.pdf [accessed on: 21/08/2017]
[98] Ibid.

> "it is better to have the Government providing the identification service. Where there is access to remedies, fair procedures and rights and the ability to see clearly what is happening with my data, it would be better if the State was providing that service.
>
> … If a decision is taken that the State will not provide them in the future - the State is not in a position to provide them at present - there is the default position and we will have to use social media or some specialist provider to provide identification services. I do not believe that is good".

Regarding the protective oversight for individuals resulting from who provides the identification services, he explained that if the State provides identification services individuals will have many protections such as judicial review and fair procedure. However, if private bodies are providing such services then protective oversight will be lower, individual's protective oversight options will be limited to either bringing an action before the courts or complaining to the DPC.[100]

Ibec in its written submission called for clarification on whether the State or private bodies will implement the identification services required for the purposes of the GDPR. Ibec stated:[101]

> "[c]larification is required on whether the state intends to implement the identification service necessary under the GDPR to, for example, differentiate between adults [and] children. If the onus falls to the market, and not the state, then this should be clarified sooner rather than later to allow solutions to be readied in time by businesses for GDPR enactment in May 2018."

Recommendation 13: Provision of identification services

The Committee recommends that the Government clarify as soon as possible whether the State OR private bodies (Google, Facebook, etc) will provide identification services online to distinguish between adults and children for data protection purposes.

[99] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Dr Denis Kelleher (Barrister-at-Law), at p.4 (21/06/2017). Available at: http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/WebAttachments.nsf/($vLookupByConstructedKey)/committees~20170621~JUJ/$File/Daily%20Book%20Unrevised.pdf [accessed on: 21/08/2017]

[100] Ibid., at p.8

[101] Ibec, '*Ibec submission to the pre-legislative scrutiny of the General Scheme of Data Protection Bill 2017*', at p.14 (05/07/2014)

6. Sanctions

The GDPR provides for administrative fines and compensation for individuals for the processing of personal data that breaches the GDPR.

6.1. Administrative Fines

This section will set out the administrative fines provisions in the GDPR and the General Scheme and summarise stakeholders' evidence during the PLS hearings concerning the application of administrative fines to public bodies.

- **General Data Protection Regulation**

Article 83 of the GDPR provides general conditions for the imposition of administrative fines by supervisory authorities for breaches of certain data protection laws. At the maximum end, administrative fines can be up to €20 million or 4% of total worldwide annual turnover for the previous year (whichever is higher). Article 83(7) provides that Member States may set down rules on whether, and to what extent, administrative fines may be imposed on public authorities and bodies.

- **General Scheme**

Head 23 of the General Scheme, entitled "*Imposition of administrative fines on public authorities and bodies (Article 83(7))"*, provides that an administrative fine may be imposed on a public authority or body ('public body') for an infringement of the GDPR "arising from its activity as an undertaking". An undertaking is defined by reference to s.3 of the *Competition Act 2002*.[102]

Public bodies engaged in undertakings

The Explanatory Notes to Head 23 of the General Scheme provide that:

> "[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."

[102] Section 3 of the *Competition Act 2002* defines "undertaking" as meaning "a person being an individual, a body corporate or an unincorporated body of persons engaged for gain in the production, supply or distribution of goods or the provision of a service". Available at: http://www.irishstatutebook.ie/eli/2002/act/14/enacted/en/html [accessed on 06/09/2017]

It goes on to say using the competition law model of an "undertaking" is one possible approach. Citing Irish case law, it suggests that each activity of the public body, and the circumstances in which that activity is performed, may be analysed separately.

The Explanatory Notes to Head 23 of the General Scheme cite the two cases - *Medicall Ambulance Service Ltd v HSE*[103] and *Lifeline Ambulance Services Ltd v HSE*[104] - in support of using an undertaking to delineate between categories of public bodies. In *Medicall*, the HSE was acting as an undertaking when providing ambulance services to private patients as it was in competition with private operators. Whereas in *Lifeline* the HSE was not acting as an undertaking when providing ambulance services to public patients as it was providing the service in the public interest and not for gain.

- **Evidence to the Committee**

Mr Carroll stated the imposition of administrative fines on public bodies when acting as undertaking "will help to ensure fairness in cases in which both public and private bodies are providing similar goods and services".[105]

The Commissioner observed in evidence that "[i]t is a serious matter of concern" for the office that administrative fines would not be imposed on all public bodies.[106] Failure to do so would cancel out the deterrent effect of such fines. The Commissioner stated that:[107]

> "the DPC's firm position is that all organisations should be treated in the same way without distinction as to whether they are engaged in commercial activity or any other activity, so that, in principle, all public bodies and authorities are capable of being fined where they infringe the GDPR. If this is not the case, the deterrent value of administrative fines in the public sector would be nullified."

The Commissioner went on to say that applying administrative fines to all public bodies is vital to encourage higher levels of compliance:[108]

> "[b]ased on its experience in regulating the public sector to date, the DPC's position is that making all public authorities/ bodies liable to administrative fines is crucial if we are to encourage greater levels of compliance with data protection law amongst public authorities and public bodies than that sector has traditionally demonstrated."

In evidence to the Committee, the Commissioner explained the deterrent nature of fines:[109]

---

[103] *Medicall Ambulance Service Ltd v HSE* [2011] IEHC 76 (available at: http://www.bailii.org/cgi-bin/format.cgi?doc=/ie/cases/IEHC/2011/H76.html [accessed on 29/05/2017])
[104] *Lifeline Ambulance Services Ltd v HSE* [2012] IEHC 432 (available at: http://www.bailii.org/cgi-bin/format.cgi?doc=/ie/cases/IEHC/2012/H432.html [accessed on 29/05/2017])
[105] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion'*, evidence of Seamus Carroll, at p.5 (14/06/2017)
[106] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion'*, evidence of Helen Dixon, at p.19 (14/06/2017)
[107] Opening Statement of the Data Protection Commissioner, 'General Scheme of the Data Protection Bill 2017' (14/06/2017) at p.7
[108] Ibid.

> "[t]he purpose of the punitive fines provided for in the new law is to act as a deterrent to all types of organisations, and we see no basis upon which public authorities would be excluded, particularly given that arguably higher standards in the protection of fundamental rights are demanded of those entities."

Mr McGarr stated that there does not seem to be any reasons for exempting public bodies from administrative fines and recommended that Article 83(7) of the GDPR is implemented without any restrictions:[110]

> "[i]t seems that there is very little by way of compelling reasons for providing this exemption for the State bodies. Certainly there is nothing set out in the explanatory note as to why State bodies ought to be exempt as a matter of policy. There are very clear reasons for having State bodies subject to the same regulatory system as the rest of civil society. Our recommendation is that it would be better if article 83(7) was implemented without any restrictions on the administrative responses available to the Data Protection Commissioner, including such fines as the commission found appropriate in respect of breaches of citizens' personal data privacy."

Mr McGarr went on to say:[111]

> "[t]he result of that positive statement [that the State shall be liable for fines when acting as an undertaking] is to create, although unstated in the [H]ead, a requirement that the State shall not be liable under any other circumstances. There is no justification provided for in the [H]eads of the Bill that we can examine and address, but it certainly does not seem to me that it would be in line with best policy practice to allow the State to exempt itself from the provisions of what are very significant citizenry rights protection legislation."

Dr Kelleher in evidence stated that he had an issue with fines in that they detract "from the real deterrence for public bodies". In particular he cited the possibility that the DPC may declare that personal data has been illegally processed and that an individual may sue for damages where a public body processes without a proper legal basis.[112]

Dr Kelleher questioned whether the possibility of the imposition of an administrative fine on public bodies was an effective deterrent. His basis for questioning its effectiveness relates to the fact the DPC and public bodies are in receipt of funding from the State. He said the imposition of fine by the

---

[109] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion'*, evidence of Helen Dixon, at p.19 (14/06/2017)
[110] Ibid., at p.6
[111] Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Simon McGarr, at p.11 (05/07/2017)
[112] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Dr Denis Kelleher (Barrister-at-Law), at p.11 (21/06/2017). Available at: http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/WebAttachments.nsf/($vLookupByConstructedKey)/committees~20170621~JUJ/$File/Daily%20Book%20Unrevised.pdf [accessed on: 21/08/2017]

DPC on a public body was a "circular transaction", in that the money for the fine comes from State funds and goes back into State funds.[113]

Mr McGarr said the circular nature of administrative fines on public bodies results in them being "cost-neutral".[114] He went on to say that by only applying administrative fines on public bodies acting as an undertaking creates an exemption for other public bodies:[115]

> "[t]he effect of this exemption is to make sure [public bodies] are not liable to fines on all other occasions when they are not acting as an undertaking. The result is to exempt public bodies and State agencies from administrative fines. The committee will have heard from the Data Protection Commissioner and other witnesses already. I echo them in saying that this is a very unwise course of action for the State to have taken."

In highlighting the value of applying administrative fines on public bodies, Mr McGarr stated the build up of fines could act as an indicator that there are problems with how public bodies are processing personal data:[116]

> "State agencies will not have the same level of accountability as commercial bodies. Between State agencies, a tally in respect of fines over the course of years is a very good initial indicator of any structural or institutional difficulty that may be arising. Such a difficulty is easy to see as the fines build up, should there be repeated fines, and therefore it is less likely that long-term structural difficulties will develop."

Potential effects of assessing whether public bodies are acting as an undertaking

The Commissioner in evidence described how having to assess whether a public body was acting as an undertaking would result in an additional workload for the DPC that would divert the DPC's resources from its core data protection role.[117]

Mr McGarr in evidence supported the position of the DPC that assessing whether a public body was acting as an undertaking could divert resources from its data protection role due to the complex legal test this assessment would require. Mr McGarr stated:[118]

> "[t]he proposed provision requires a legally very complex test to be carried out on each occasion that the Data Protection Commission thinks it is necessary to do so, before any administrative fines could be levied. On every occasion, there would have to be an examination of whether elements of public authority were acting as an undertaking before an administrative fine could be levied. In the explanatory note to the heads of the Bill, it is

[113] Ibid., at p.3 & p.11
[114] Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Simon McGarr, at p.6 (05/07/2017)
[115] Ibid., at pp.5-6
[116] Ibid., at p.6
[117] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion'*, evidence of Helen Dixon, at p.19 (14/06/2017)
[118] Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Simon McGarr, at p.6 (05/07/2017)

> acknowledged that this is a complicated matter. It cannot be said that a particular State body is an undertaking in all its activities. The example given in the explanatory note is that the HSE in the provision of ambulances is sometimes an undertaking and is sometimes not."

In addition, he said such assessments by the DPC introduce the possibility of legal challenges by public bodies to a finding that it is acting as undertaking. He stated that:[119]

> "[t]his is a high legal threshold for the regulator to have to get over every time it must decide whether it is possible to exercise legal powers. It also introduces the potential of a challenge by the public body to every such effort to exercise those powers, in respect of whether it is acting as an undertaking."

Ibec, in its written submission, expressed reservations about only applying administrative fines to public bodies acting as an undertaking. Ibec stated:[120]

> "Ibec has some reservations about the proposal to only impose administrative fines on public authorities insofar as they are acting as undertakings. Whether a body is acting for gain or not, it seems more equitable to apply the same rules to the private and public sector."

Recommendation 14: Administrative fines

The Committee recommends that fines be administered to public bodies in breach of the new data protection legislation where appropriate, to encourage compliance with data protection provisions in the new legislation.

6.2. Right to Receive Compensation

This section will set out the compensation provisions in the GDPR, the Law Enforcement Directive and the General Scheme for breaches of the data protection law. It will also summarise stakeholders' evidence during the PLS hearings questioning whether the right to receive compensation in the GDPR needs to be provided for in the proposed legislation.

- **General Data Protection Regulation**

Article 82 of the GDPR provides that a person who suffers material or non-material damage, e.g. where they suffered distress or humiliation[121] due to an infringement of the GDPR, has a right to receive compensation from the data controller or processor.

[119] Ibid.
[120] Ibec, '*Ibec submission to the pre-legislative scrutiny of the General Scheme of Data Protection Bill 2017*', at p.8 (05/07/2014)
[121] Helen Dixon (Data Protection Commissioner), *With clock ticking on new EU data protection law, companies must act now*, Irish Independent (25/05/2017) (available at: https://global.factiva.com/redir/default.aspx?p=sa&an=IINM000020170525ed5p0002w&cat=a&ep=asi&NS=18&AID=9HOU003400 [accessed on 31/05/2017])

- **Law Enforcement Directive**

In addition to the right to receive compensation in the GDPR, the Law Enforcement Directive also provides a right to receive compensation for material and non-material damages. Article 56 of the Directive provides that Member States must provide that any person who has suffered material or non-material damage resulting from the unlawful processing of personal data, or an infringement of national law transposing the Directive, has a right to receive compensation from the data controller or other national competent authority.

- **General Scheme**

Head 58 in Part 4 of the General Scheme, entitled "*Right to compensation*", provides that a person who suffers material or non-material damage due to an infringement of Part 4 has a right to receive compensation from the competent authority or data processor for damage or distress suffered. Part 4 of the General Scheme transposes the Law Enforcement Directive.

Part 6 of the General Scheme, entitled "*Miscellaneous Provisions*" concerns, among other matters, the right of data subjects to an effective judicial remedy. Head 91(3) in Part 6 of the General Scheme, entitled "*Judicial Remedy*", provides that:

> "[i]n a data protection action under this Head, the Circuit Court shall, without prejudice to its powers to award compensation in respect of material and non-material damage, have the power to grant relief by means of injunction or declaratory orders."

Under the General Scheme compensation can only be awarded by the courts, e.g. the DPC will not have the power to award compensation.[122] In evidence the Commissioner explained that the data protection authorities are not, nor will they be, "full blown ombudsmen" and that they do not have the power to order redress or compensation.[123] She went on to say that the DPC's reading of the GDPR is that "court proceedings are required to achieve that compensation".[124] She also stated that the right to receive compensation will be independent of the DPC's enforcement powers.[125]

Is there a need for an explicit right to receive compensation for the purposes of the GDPR?

Dr Eoin O'Dell (Associate Professor, School of Law, Trinity College Dublin) queried whether the wording of Article 82(1) of the GDPR was "sufficiently clear, precise and unconditional" enough to be horizontally effective e.g. it is not clear whether an individual can invoke the right against another

[122] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion'*, evidence of Seamus Carroll, at p.10 (14/06/2017)
[123] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion'*, evidence of Helen Dixon, at p.20 (14/06/2017)
[124] Ibid.
[125] Opening Statement of the Data Protection Commissioner, 'General Scheme of the Data Protection Bill 2017' (14/06/2017) at p.8

individual without national legislation giving further effect to the right.[126] Writing about the General Scheme, he noted the German law giving effect to the GDPR contains "an explicit provision giving effect to Article 82 GDPR".[127]

- **Evidence to the Committee**

Mr Carroll stated the Department are still reviewing a number of policy issues. In addition, consultations with the European Commission, the Attorney General's Office and the Data Protection Commissioner are on-going, including matters relating to compensation.[128]

Mr Carroll said the Department was aware of the German law, however, he went on to highlight some uncertainty as to whether the right to receive compensation can be provided for in Irish law. He stated:[129]

> "[w]e are aware of the provision in German law explicitly giving effect to the right to receive compensation under the GDPR. One of the difficulties we face here is whether, when an article of the GDPR does not make specific reference to the possibility of national law, national law is nonetheless possible. As I mentioned towards the end of my presentation, this question - namely, whether further effect or some kind of flanking measure to Article 82 may be included in our Bill - is one of the questions about which we are in consultation with the Attorney General at present. The question is, therefore, under active consideration."

Dr Kelleher stated that he does not believe an explicit provision is needed to give effect to the right to compensation in Article 82 of the GDPR.[130]

However, evidence from other stakeholders during PLS Hearings recommended the proposed legislation provide an explicit right to receive compensation. For example, both **Mr McGarr and Dr O'Dell** stated that the use of "shall" in Article 82 of the GDPR indicates that a Member State is required to do something further to give full effect to the provision.[131]

---

[126] Dr Eoin O'Dell, 'Submission on the General Scheme of the Data Protection Bill 2017 to the Committee on Justice and Equality' (n.d.)

[127] Professor Eoin O'Dell (cearta.ie), *The Heads of an Irish Bill to ensure GDPR compliance are very welcome, but they raise questions about repeals and compensation* (12/05/2017) (available at: http://www.cearta.ie/2017/05/the-heads-of-an-irish-bill-to-ensure-gdpr-compliance-are-very-welcome-but-they-raise-questions-about-repeals-and-compensation/ [accessed on 12/06/2017])

[128] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion'*, evidence of Seamus Carroll , at p.7 (14/06/2017)

[129] Ibid., at p.13

[130] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Dr Denis Kelleher (Barrister-at-Law), at p.5 (21/06/2017). Available at: http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/WebAttachments.nsf/($vLookupByConstructedKey)/committees~20170621~JUJ/$File/Daily%20Book%20Unrevised.pdf [accessed on: 21/08/2017]

[131] Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Simon McGarr, at p.7 (05/07/2017) and Dr Eoin O'Dell, '*Submission on the General Scheme of the Data Protection Bill 2017 to the Committee on Justice and Equality'* (n.d.)

Mr McGarr and Dr O'Dell similarly stated that Head 91 of the General Scheme recognises or assumes a right of action before the courts, but does not provide an explicit right to compensation.[132] Both stakeholders recommended the proposed legislation give explicit recognition to the right to receive compensation for claims for compensation under both Article 82of the GDPR and Article 56 of the Law Enforcement Directive.[133]

Dr O'Dell additionally stated that such provision should provide that such actions are founded on tort and that the word "damages" should be used in place of "compensation". Other than that, he said the provision of the right should use as much of the language of Article 82 of the GDPR and Article 56 of the Law Enforcement Directive as possible.[134]

Furthermore, Dr O'Dell submitted that it would be better that the proposed legislation provide an explicit right to receive compensation rather than leaving the matter "to the vagaries of litigation to – and in – the CJEU" and hoping that the CJEU finds the right is directly effective.[135] If the CJEU were to find that the right was not directly effectively, he stated the failure to enact such legislation could leave the State vulnerable to claims for damages from individuals who have suffered a loss as a result of not providing the necessary national legislation.[136]

Mr McGarr in evidence also alerted that the failure to give explicit recognition to the right to receive compensation could leave a question mark over whether the State has complied with its obligation to provide for such a right, and it could leave the State open to claims for compensation "that would have otherwise fallen on private third parties who were breaching the data protection rights".[137]

Recommendation 15: Right to receive compensation

The Committee recommends that an explicit right to compensation be outlined in the new legislation for breaches of data protection provisions. A consultation with the DPC, Office of the Attorney General, the European Commission could assist in the drafting of such a provision.

[132] Ibid.
[133] Ibid.
[134] Dr Eoin O'Dell, '*Submission on the General Scheme of the Data Protection Bill 2017 to the Committee on Justice and Equality*' (n.d.)
[135] Ibid.
[136] Ibid.
[137] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Simon McGarr, at pp.6-7 (05/07/2017)

6.3. Representation of data subjects by not-for-profit bodies and 'class actions' for data protection beaches

This section will set out stakeholders' evidence during the PLS hearings concerning Representation of data subjects by not-for-profit bodies in Article 80 of the GDPR. It also sets out stakeholders' evidence that 'class actions', where data subjects can mandate certain not-for-profit bodies to represent them as a group in data protection proceedings, are provided for in Article 80 of the GDPR. The General Scheme is silent as to both these aspects of the GDPR.

- **General Data Protection Regulation**

Article 80(1) of the GDPR concerning representation of data subjects provides:

> "[t]he data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77 [the right to lodge a complaint with the supervisory authority (the DPC)], 78 [the right to an effective judicial remedy against the supervisory authority] and 79 [the right to an effective judicial remedy against a data controller or data processor] on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law."

Article 80(2) of the GDPR also provides that Member States "may provide" that any such body, organisation or association has a right to lodge a complaint in that Member State with the data protection authority independently of a data subject's mandate where it considers that a data subjects rights under the GDPR have been infringed.

- **Evidence to the Committee regarding representation by not-for-profit bodies**

Dr McIntyre stated that Article 80 of the GDPR contains a 'mandatory provision' requiring Member States to permit individuals to mandate not-for-profit bodies, organisations or associations ('not-for-profit bodies') to lodge a complaint on his or her behalf and to exercise data subjects rights in Articles 77, 78 and 79 on his or her behalf.[138] However, he went on to say that Head 91 of the General Scheme, concerning judicial remedy, is silent as to this obligation.

[138] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Dr TJ McIntyre, at p.3 (05/07/2017)

Dr McIntyre recommended the proposed legislation be modified to include provisions permitting individuals to mandate not-for-profit bodies to lodge a complaint on his or her behalf.[139]

In addition to the mandatory provision, Dr McIntyre stated that Article 80 of the GDPR has two discretionary provisions. The discretionary provisions are that Member States may:[140]

- permit individuals to mandate not-for-profit bodies to seek compensation on his or her behalf; and
- provide that not-for-profit bodies can independently bring actions without having to be mandated by an individual data subject to do so.

He went on to say that the Heads of Bill are silent as to these two discretionary provisions. [141]

Dr McIntyre stated that it is "very important" for practical and principled reasons that Ireland implement the two discretionary provisions in Article 80 of the GDPR.[142]

Regarding the practical reasons for implementing the discretionary provisions, Dr McIntyre stated that failing to provide for the two discretionary provisions would result in a "multiplicity of claims being brought before the courts that the courts simply are not equipped to address".[143]

Regarding the principled reasons for implementing the discretionary provisions, Dr McIntyre stated that failing to do so may result in a gap in implementation. He gave the example where a data breach involves sensitive personal information, despite being identifiable and suffering harm, an individual might be "very reluctant or unable to come forward".[144] In other situations individuals may not "be in a position to bring a complaint or action in respect of the matter".[145] He noted that the Irish High Court, in the context of legal proceedings challenging data retention laws, acknowledged "that it was important that Digital Rights Ireland would be able to bring an *action popularis*, an action on behalf of the wider population".[146]

Dr McIntyre stated that DRI recommends the proposed legislation is amended to provide:[147]

- that a data subject can mandate a not-for-profit body to seek compensation on his or her behalf; and

[139] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Dr TJ McIntyre, at p.3 (05/07/2017)
[140] Ibid., at p.3
[141] Ibid.
[142] Ibid.
[143] Ibid.
[144] Ibid., at pp.3-4
[145] Ibid., at p.4
[146] Ibid.
[147] Dr TJ McIntyre, '*Joint Committee on Justice and Equality, Wednesday 5 July 2017 Comments on the General Scheme of Data Protection Bill (May 2017 draft)*' (05/07/2017), at p.4

- that a properly qualified not-for-profit body has the right to lodge a complaint or seek an injunction against a control/processor if it considers that the rights of a data subject have been infringed.

Recommendation 16: Representation by not-for-profit bodies, organisations or associations in data protection actions

The Committee recommends that provision be contained in the proposed legislation for an individual to mandate a properly qualified not-for-profit body, organisation or association, on the data subject's behalf, to lodge a complaint and to exercise their rights under Articles 77 (the right to lodge a complaint with the supervisory authority), 78 (the right to an effective judicial remedy against the supervisory authority) and 79 (the right to an effective judicial remedy against a data controller or data processor) of the GDPR. This provision should also cover the right of an individual to mandate a properly qualified not-for-profit body, organisation or association to seek compensation on his or her behalf.

In addition, there is also merit in giving consideration to providing that a properly qualified not-for-profit body, organisation or association to can independently bring actions that there have been breaches of data protection law under the GDPR or the proposed legislation, without having to be mandated by an individual data subject to do so.

- **Evidence to the Committee regarding 'class actions'**

A related issue to representation of individuals by not-for-profit bodies provided for in Article 80 of the GDPR is the issue of 'class actions', whereby such bodies can represent a multiplicity of data subjects in a data protection action. The General Scheme is silent as to class actions.

Dr Kelleher in his written statement stated that Article 80 of the GDPR concerning the representation of data subjects by a not-for-profit body "seems to effectively provide for class actions "where provided for by Member State law"".[148] He stated that at present "[t]he Irish Rules of Court do not provide for such class actions at the present time, though it does provide for representative actions".[149,150]

Despite the Irish Rules of Courts not providing for class actions, Dr Kelleher stated:[151]

> "I would be surprised if one does not see lawyers bringing forward claims stating that they want to bring forward a class action and testing elements of that, and stating under Article 80 of the GDPR they are entitled to bring forward class actions and they want to bring forward those class actions."

[148] Dr Denis Kelleher BCL, BL '*Submission on Heads of Data Protection Bill 2017*', at p.6 (20/06/2017)
[149] Ibid.
[150] As summarised in the Law Reform Commission 'Consultation Paper on Multi-party Litigation (Class Action)', Order 15 rule 9 of the *Rules of the Superior Courts 1986* provides a mechanism that "enables large numbers of persons to be joined to a legal action as represented parties". The Paper states that in Ireland, representative action has only been used "a handful of cases" due limitations surrounding its operation. See Law Reform Commission (2003), 'Consultation Paper on Multi-party Litigation (Class Action)' (LRC - CP 25 - 2003) at para. 1.03. Available at: http://www.lawreform.ie/_fileupload/consultation%20papers/cp25.htm [accessed on 05/09/2017]
[151] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Dr Denis Kelleher (Barrister-at-Law), at p.11 (21/06/2017). Available at: http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/WebAttachments.nsf/($vLookupByConstructedKey)/committees~20170621~JUJ/$File/Daily%20Book%20Unrevised.pdf [accessed on: 21/08/2017]

He concluded that:[152]

> "[o]ne way or another, one will find oneself with some sort of representative or class action being brought before the courts."

In the context of his evidence relating to the two discretionary provisions concerning not-for-profit representation in Article 80 of the GDPR, **Dr McIntyre** stated that "[t]he GDPR gives us the option to effectively consolidate these cases if we allow people to nominate not-for-profit bodies to act on their behalf to bring a single action".[153]

Ibec, in its written submission, stated that the provision of class actions should be subject to a public consultation:[154]

> "[c]lass actions are not possible today in the State and we submit that the provision for class actions would be a significant development for Irish law. Any such proposed development and would require detailed consultation if consideration is being given to its introduction as part of the DP Bill or otherwise."

Recommendation 17: Class actions

The Committee recommends that provision for 'class actions', or for similarly grouped plaintiffs to be heard together, should be explicitly provided for in the proposed legislation.

[152] Ibid.
[153] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Dr TJ McIntyre, at p.3 (05/07/2017)
[154] Ibec, '*Ibec submission to the pre-legislative scrutiny of the General Scheme of Data Protection Bill 2017*', at pp.13-14 (05/07/2014)

7. Restrictions to the rights and obligations in the GDPR

This section sets out stakeholders' recommendations made during PLS on the General Scheme to amend the proposal in Head 20 of the General Scheme, entitled "*Restrictions on exercise of data subjects rights (Article 23)*", permitting Ministers to restrict certain data protection rights and obligations by Regulations.

- **General Data Protection Regulation**

Article 23 of the GDPR provides that Member States may, by way of legislative measure, restrict the scope of specified rights and obligations in the GDPR. The adoption of these restrictions is limited to the purposes set out in Article 23(1) such as national security or public security.[155] Restrictions must respect the "essence of the fundamental rights and freedoms" of data subjects and be "necessary and proportionate measure[s] in a democratic society to safeguard" the purposes set out in Article 23(1).

The rights and obligations which may be restricted are those set down in Articles 12 to 22, 34 and 5 (in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22) of the GDPR.[156]

Article 23(2) of the GDPR provides that legislative measures restricting the scope of specified rights and obligations in the GDPR must contain certain specified measures, where relevant.[157]

[155] The full list of purposes for which the rights and obligations above may be restricted in Article 23(1) of the GDPR are: "(a) national security; (b) defence; (c) public security; (d) 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; (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); (i) the protection of the data subject or the rights and freedoms of others; (j) the enforcement of civil law claims."

[156] The rights and obligations in in Articles 12 to 22, 34 and 5 of the GDPR are: information to be provided to data subjects under Articles 12 to 14; right of access in Article 15; right to rectification of inaccurate personal data in Article 16; right to erasure of personal data ("right to be forgotten") in Article 17; right to restriction of processing of personal data in Article 18; obligation on data controllers in Article 19 to notify third party recipients of personal data that the data has been rectified, erased or its processing has been restricted; right to data portability in Article 20; right to object to the processing of personal data in Article 21; right not to be subject to automated individual decision-making, including profiling in Article 22; obligation on data controllers to communicate a personal data breach to a data subject in Article 34; and data processing principles in Article 5.

[157] Legislative measures restricting the scope of specified rights and obligations in the GDPR must contain *at least* the following specific measures, where relevant: "(a) the purposes of the processing or categories of processing; (b) the categories of personal data; (c) the purposes of the processing or categories of processing; (d) the categories of personal data; (e) the scope of the restrictions introduced; (f) the safeguards to prevent abuse or unlawful access or transfer; (g) the specification of the controller or categories of controllers; (h) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; (i) the risks to the rights and freedoms of data subjects; and (j) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction."

- **General Scheme**

Head 20 of the General Scheme, entitled "*Restrictions on exercise of data subjects rights (Article 23)*", proposes to provide Ministers broad discretionary power, by Regulations, to restrict specified rights and obligations in the GDPR where necessary to "safeguard important objectives of general public interest".

Head 20(1) of the General Scheme proposes that Ministers may, by Regulations, following consultation with the relevant Minister and Data Protection Commission, restrict the rights and obligations in Articles 12 to 22, 34 and 5 (in so far as its provisions correspond to such rights and obligations) of the GDPR. Head 20(2) proposes a long, non-exhaustive list of important public interest objectives for which the rights and obligations in the GDPR may be restricted.[158]

Head 20(3) of the General Scheme proposes that Regulations restricting the exercise of data subjects' rights must contain specified provisions, where relevant.[159] The General Scheme does not provide any further information regarding what specific exemptions and measures made in Regulations under this Head may contain.

[158] These are: "(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."

[159] These are: "(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."

- **Evidence to the Committee**

Dr McIntyre in evidence stated that DRI were concerned about the potential "far-reaching power" Head 20 of the General Scheme seems to confer on Ministers to restrict data protection rights and obligations by way of regulations. [160] In a supplemental written submission, Dr McIntyre said that:[161]

> "it seems to DRI that Head 20(1) – by providing a largely open-ended power to *any* Minister to make regulations in *any* area restricting *any* data subject rights on the basis of *any* "important objectives of general public interest" – is extremely problematic." (emphasis in original)

He went on to query whether the enabling provision in Head 20 of the General Scheme was too "open-ended" as to comply with the domestic constitutional requirement under with Article 15.2 of the Constitution of Ireland concerning delegated legislation. He questioned whether Head 20 would meet the principles and policies test established in case law[162] whereby delegated legislation must do no more than merely giving effect to the principles and policies in the Act itself.[163] Dr McIntyre stated that:[164]

> "[i]n this case, however, Head 20 provides for the restriction of data subject rights on the basis of an "intentionally non-exhaustive" list which includes any "important objectives of general public interest". It is difficult to see that this open-ended power meets the domestic constitutional requirements of Article 15.2".

In addition to the concerns raised by Dr McIntyre as to whether Head 20 of the General Scheme would meet domestic constitutional law requirements, **Mr McGarr** queried whether it would meet EU law requirements. He said that under the case law of the CJEU the State does not have "a free hand" to restrict matters that are underpinned by the EU Charter, when providing for such restrictions in legislation States must "give consideration to the questions of necessity or proportionality".[165]

Mr McGarr went on to query whether the provisions of Head 20 of the General Scheme would, if enacted, withstand a challenge before the CJEU.[166] He emphasised that the State has received

[160] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Dr TJ McIntyre, at p.4 (05/07/2017)
[161] Dr TJ McIntyre, '*Supplemental Comments on the General Scheme of Data Protection Bill (May 2017 draft)*', at p.1 (05/07/2017)
[162] *Cityview Press v An Comhairle Oiliúna* [1980] IR 381
[163] Dr TJ McIntyre, '*Supplemental Comments on the General Scheme of Data Protection Bill (May 2017 draft)*', at p.1 (05/07/2017)
[164] Ibid.
[194] Oireachtas Joint Committee on Justice and Equality, *'General Scheme of Data Protection Bill: Discussion (Resumed)'*, evidence of Simon McGarr, at p.8 (05/07/2017)
[166] Ibid.

guidance from the DPC that data-sharing exemptions should be done by way of primary legislation:[167]

> "I know the Data Protection Commissioner has issued a guidance note to State agencies on data sharing following the Bara judgment and the State has received guidance from its legal advisers in respect of the desirability of passing such data-sharing exemptions from the [D]ata [P]rotection [D]irective by way of primary legislation. It is important that if the State is to provide for certain matters to be dealt with and if primary legislation is required in order to ground an exemption from the [D]ata [P]rotection [D]irective on a lawful basis, which is a provided for in the directive, it should not provide for non-primary legislative means. It seems like a recipe for challenge and, in all likelihood, a recipe for the Data Protection Commissioner to have to deal with a repeated number of complaints and challenges to actions of the State."

Dr McIntyre in evidence noted the Explanatory Notes to Head 20 of the General Scheme stated that:

> "the Department acknowledges it would be desirable for Departments to introduce limitations on these rights by means of primary legislation but it suggests it is nevertheless necessary to have a residual power by means of statutory instrument to introduce these exceptions".[168]

In his supplemental written submission, Dr McIntyre stated that DRI recommends that:[169]

> "[w]here necessary, specific statutory powers should be put in place to make regulations restricting data subject rights, and that Head 20(1) should be deleted."

If Head 20(1) is retained, Dr McIntyre stated that DRI recommends the power should be narrowed and subjected to additional safeguards. He stated:[170]

> "in the event Head 20(1) is retained, it should be modified to ensure that the power to make regulations under this section is a residual one, to be used only where there is no other specific statutory power (to avoid evasion of restrictions which might apply under those other powers) and subject to additional safeguards such as a requirement of a positive resolution of both Houses of the Oireachtas before the regulations come into force, a sunset clause limiting the duration of Head 20(1) to a transitional period following the adoption of the Act, or a sunset clause limiting the duration of regulations made under this provision."

Recommendation 18: Restrictions to the rights and obligations in the GDPR where necessary to "safeguard important objectives of general public interest"

The Committee recommends that restrictions to the rights of citizens under the GDRP be limited in scope and sufficient safeguards should be put in place in the new legislation to ensure that the ability to restrict data protection rights is not abused by the state.

[167] Ibid.
[168] Oireachtas Joint Committee on Justice and Equality, 'General Scheme of Data Protection Bill: Discussion (Resumed)', evidence of Dr TJ McIntyre, at p.4 (05/07/2017)
[169] Dr TJ McIntyre, '*Supplemental Comments on the General Scheme of Data Protection Bill (May 2017 draft)*', at p.2 (05/07/2017)
[170] Ibid.

Recommendations

1) Repeal of the Data Protection Acts

The Committee recommends that the old *Data Protection Acts* should be repealed in their entirety. Provisions within these Acts which may require retention can be preserved by enacting stand-alone legislation.

2) Legislate separately for the Law Enforcement Directive

The Committee recommends that the Law Enforcement Directive be transposed in separate legislation to the General Scheme addressed in this report.

3) Include the GDPR text within the new legislation

The Committee recommends that the text of the GDPR be included verbatim in the proposed legislation as an appendix. This will help ensure transparency and consistency when the legislation is enacted.

4) Structure of the proposed legislation

Following the enactment of the proposed legislation, consideration should be given to producing an administrative consolidated version of the GDPR with the corresponding national law provisions. This will result in individuals only having to read through one document when ascertaining their data protection rights and obligations. This would make data protection law more accessible, and aid the safeguarding of citizens' fundamental right to protection of their personal data.

5) Digital age of consent

The Committee recommends that the digital age of consent be set at 13 years of age. The Committee also recommends that this age of consent be reviewed at appropriate intervals to ensure it remains suitable as technology evolves.

6) Consultation with children

The Committee recommends that a detailed consultation take place with children of all ages to ascertain their views on the proposed measures for data protection.

7) Definition of 'child'

The Committee recommends that a definition of who is a 'child' be included in the proposed legislation. The definition of 'child' – as per Article 1 of the UNCRC – should include every person below 18 years of age.

8) Definition of 'the holder of responsibility'

The term 'holder of parental responsibility' in Head 16 is not defined within the proposed legislation, and the Committee recommends that a broad definition of parental responsibility be applied, to include natural or court-appointed responsibility.

9) Definition of 'preventative or counselling services'

The Committee recommends that a broad range of defined preventative and counselling services be provided to children to enable them to deal with data protection issues when they so need.

10) Right to be forgotten and children

Owing to their particular vulnerability online, the Committee recommends that children be granted a specific and explicit right to be forgotten online.

11) Policy framework and educational programme to assist children in exercising their digital rights before they reach the digital age of consent

The Committee recommends that a policy framework and an associated educational programme be implemented to assist children in exercising their digital rights before they reach the digital age of consent.

12) Additional safeguards for the processing of sensitive personal data

The Committee recommends that additional safeguards be implemented to ensure that the processing of a child's sensitive data under Head 18 is conducted in a safe manner.

13) Provision of identification services

The Committee recommends that the Government clarify as soon as possible whether the state OR private companies will be responsible for providing identification services online to distinguish between adults and children for data protection purposes.

14) Administrative fines

The Committee recommends that fines be administered to public bodies in breach of the new data protection legislation where appropriate, in order to encourage compliance with the new legislation.

15) Right to receive compensation

The Committee recommends that an explicit right to compensation be outlined in the new legislation for breaches of data protection provisions. A consultation with the Data Protection Commissioner, Office of the Attorney General, and the European Commission could assist in the drafting of such a provision.

16) Representation by not-for-profit bodies, organisations or associations data protection actions

The Committee recommends that provision be contained in the proposed legislation for an individual to mandate a properly qualified not-for-profit body, organisation or association, on the data subject's behalf, to lodge a complaint and to exercise their rights under Articles 77 (the right to lodge a complaint with the supervisory authority), 78 (the right to an effective judicial remedy against the supervisory authority) and 79 (the right to an effective judicial remedy against a data controller or data processor) of the GDPR. This provision should also cover the right of an individual to mandate a properly qualified not-for-profit body, organisation or association to seek compensation on his or her behalf. In addition, there is also merit in giving consideration to providing that a properly qualified not-for-profit body, organisation or association can independently bring actions for alleged breaches of data protection law under the GDPR or the proposed legislation, without having to be mandated by an individual data subject to do so.

17) Class actions

The Committee recommends that provision for 'class actions', or for similarly grouped plaintiffs to be heard together, should be explicitly provided for in the proposed legislation.

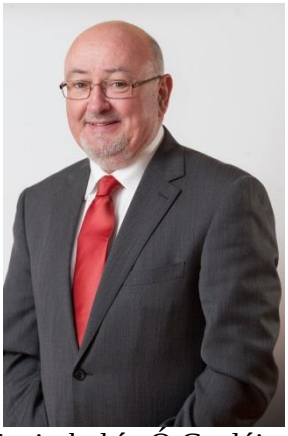
18) Restrictions to the rights and obligations in the GDPR where necessary to "safeguard important objectives of general public interest"

The Committee recommends that restrictions on the rights of citizens under the GDRP be limited in scope and that sufficient safeguards should be put in place in the new legislation to ensure that the ability to restrict data protection rights is not abused by the State.

Appendix 1 – Committee Membership

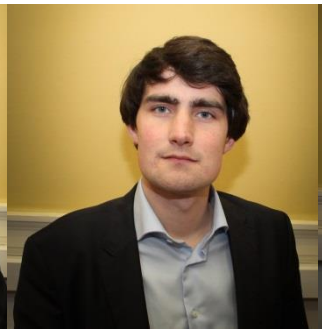
Joint Committee on Justice and Equality

Deputies

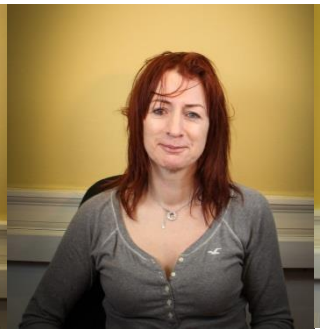


Caoimhghín Ó Caoláin TD
(SF) [Chair]

Colm Brophy TD
(FG)



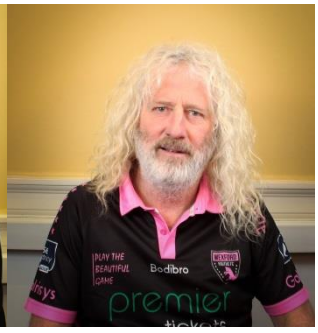
Jack Chambers TD
(FF)



Clare Daly TD
(I4C)

Alan Farrell TD
(FG)

Jim O'Callaghan TD
(FF)



Mick Wallace TD
(I4C)

Senators

Frances Black

(CEG)

Lorraine Clifford-Lee

(FF)

Martin Conway

(FG)

Niall Ó Donnghaile

(SF)

Notes:

1. Deputies nominated by the Dáil Committee of Selection and appointed by Order of the Dáil on 16th June 2016.
2. Senators nominated by the Seanad Committee of Selection and appointed by Order of the Seanad on 20th July 2016.

Appendix 2 - Orders of Reference

a) Scope and Context of Activities of Committees *(derived from Standing Orders – DSO 84, SSO 70)*

1) The Joint Committee may only consider such matters, engage in such activities, exercise such powers and discharge such functions as are specifically authorised under its orders of reference and under Standing Orders;

2) Such matters, activities, powers and functions shall be relevant to, and shall arise only in the context of, the preparation of a report to the Dáil/and or Seanad;

3) The Joint Committee shall not consider any matter which is being considered, or of which notice has been given of a proposal to consider, by the Committee of Public Accounts pursuant to Standing Order 186 and/or the Comptroller and Auditor General (Amendment) Act 1993;

4) The Joint Committee shall not consider any matter which is being considered, or of which notice has been given of a proposal to consider, by the Joint Committee on Public Petitions in the exercise of its functions under Standing Order 111A; and

   The Joint Committee shall refrain from inquiring into in public session or publishing confidential information regarding any matter if so requested, for stated reasons given in writing, by—

   (i) a member of the Government or a Minister of State, or

   (ii) the principal office-holder of a body under the aegis of a Department or which is partly or wholly funded by the State or established or appointed by a member of the Government or by the Oireachtas:

   Provided that the Chairman may appeal any such request made to the Ceann Comhairle, whose decision shall be final.

5) It shall be an instruction to all Select Committees to which Bills are referred that they shall ensure that not more than two Select Committees shall meet to consider a Bill on any given day, unless the Dáil, after due notice given by the Chairman of the Select Committee, waives this instruction on motion made by the Taoiseach pursuant to Standing Order 28. The Chairmen of Select Committees shall have responsibility for compliance with this instruction.

b) Functions of Departmental Committees (derived from Standing Orders – DSO 84A and SSO 70A)

(1) The Select Committee shall consider and report to the Dáil on-

(*a*) such aspects of the expenditure, administration and policy of a Government Department or Departments and associated public bodies as the Committee may select, and

(*b*) European Union matters within the remit of the relevant Department or Departments.

(2) The Select Committee may be joined with a Select Committee appointed by Seanad Éireann for the purposes of the functions set out in this Standing Order, other than at paragraph (3), and to report thereon to both Houses of the Oireachtas.

(3) Without prejudice to the generality of paragraph (1), the Select Committee shall consider, in respect of the relevant Department or Departments, such—

(*a*) Bills,

(*b*) proposals contained in any motion, including any motion within the meaning of Standing Order 187,

(*c*) Estimates for Public Services, and

(*d*) other matters

as shall be referred to the Select Committee by the Dáil, and

(*e*) Annual Output Statements including performance, efficiency and effectiveness in the use of public moneys, and

(*f*) such Value for Money and Policy Reviews as the Select Committee may select.

(4) Without prejudice to the generality of paragraph (1), the Joint Committee may consider the following matters in respect of the relevant Department or Departments and associated public bodies:

(*a*) matters of policy and governance for which the Minister is officially responsible,

(*b*) public affairs administered by the Department,

(*c*) policy issues arising from Value for Money and Policy Reviews conducted or commissioned by the Department,

(*d*) Government policy and governance in respect of bodies under the aegis of the Department,

(*e*) policy and governance issues concerning bodies which are partly or wholly funded by the State or which are established or appointed by a member of the Government or the Oireachtas,

(*f*) the general scheme or draft heads of any Bill

(*g*) any post-enactment report laid before either House or both Houses by a member of the Government or Minister of State on any Bill enacted by the Houses of the Oireachtas,

(*h*) statutory instruments, including those laid or laid in draft before either House or both Houses and those made under the European Communities Acts 1972 to 2009,

(*i*) strategy statements laid before either or both Houses of the Oireachtas pursuant to the Public Service Management Act 1997,

(*j*) annual reports or annual reports and accounts, required by law, and laid before either or both Houses of the Oireachtas, of the Department or bodies referred to in subparagraphs (*d*) and (*e*) and the overall performance and operational results, statements of strategy and corporate plans of such bodies, and

(*k*) such other matters as may be referred to it by the Dáil from time to time.

(5) Without prejudice to the generality of paragraph (1), the Joint Committee shall consider, in respect of the relevant Department or Departments—

(*a*) EU draft legislative acts standing referred to the Select Committee under Standing Order 114, including the compliance of such acts with the principle of subsidiarity,

(*b*) other proposals for EU legislation and related policy issues, including programmes and guidelines prepared by the European Commission as a basis of possible legislative action,

(*c*) non-legislative documents published by any EU institution in relation to EU policy matters, and

(*d*) matters listed for consideration on the agenda for meetings of the relevant EU Council of Ministers and the outcome of such meetings.

(6) Where the Select Committee has been joined with a Select Committee appointed by Seanad Éireann, the Chairman of the Dáil Select Committee shall also be the Chairman of the Joint Committee.

(7) The following may attend meetings of the Select or Joint Committee, for the purposes of the functions set out in paragraph (5) and may take part in proceedings without having a right to vote or to move motions and amendments:

(*a*) members of the European Parliament elected from constituencies in Ireland, including Northern Ireland,

(*b*) members of the Irish delegation to the Parliamentary Assembly of the Council of Europe, and

(*c*) at the invitation of the Committee, other members of the European Parliament.

(8) The Joint Committee may, in respect of any Ombudsman charged with oversight of public services within the policy remit of the relevant Department or Departments, consider—

(*a*) such motions relating to the appointment of an Ombudsman as may be referred to the Committee, and

(*b*) such Ombudsman reports laid before either or both Houses of the Oireachtas as the Committee may select: Provided that the provisions of Standing Order 111F apply where the Select Committee has not considered the Ombudsman report, or a portion or portions thereof, within two months (excluding Christmas, Easter or summer recess periods) of the report being laid before either or both Houses of the Oireachtas.

c) Powers of Committees (derived from Standing Orders – DSO 85, 114 and 116 and SSO 71, 107 and 109)

The Joint Committee has:-

(1) power to take oral and written evidence and to print and publish from time to time minutes of such evidence taken in public before the Select Committee together with such related documents as the Select Committee thinks fit;

(2) power to invite and accept oral presentations and written submissions from interested persons or bodies;

(3) power to appoint sub-Committees and to refer to such sub-Committees any matter comprehended by its orders of reference and to delegate any of its powers to such sub-Committees, including power to report directly to the Dáil;

(4) power to draft recommendations for legislative change and for new legislation;

(4A) power to examine any statutory instrument, including those laid or laid in draft before either House or both Houses and those made under the European Communities Acts 1972 to 2009, and to recommend, where it considers that such action is warranted, whether the instrument should be annulled or amended;

(4B) for the purposes of paragraph (4A), power to require any Government Department or instrument-making authority concerned to submit a Memorandum to the Select Committee explaining any statutory instrument under consideration or to attend a meeting of the Select Committee for the purpose of explaining any such statutory instrument: Provided that such Department or authority may decline to attend for stated reasons given in writing to the Select Committee, which may report thereon to the Dáil;

(5) power to require that a member of the Government or Minister of State shall attend before the Select Committee to discuss policy for which he or she is officially responsible: Provided that a member of the Government or Minister of State may decline to attend for stated reasons given in writing to the Select Committee, which may report thereon to the Dáil: and provided further that a

member of the Government or Minister of State may request to attend a meeting of the Select Committee to enable him or her to discuss such policy;

(6) power to require that a member of the Government or Minister of State shall attend before the Select Committee to discuss proposed primary or secondary legislation (prior to such legislation being published) for which he or she is officially responsible: Provided that a member of the Government or Minister of State may decline to attend for stated reasons given in writing to the Select Committee, which may report thereon to the Dáil: and provided further that a member of the Government or Minister of State may request to attend a meeting of the Select Committee to enable him or her to discuss such proposed legislation;

(6A) power to require that a member of the Government or Minister of State shall attend before the Select Committee and provide, in private session if so requested by the member of the Government or Minister of State, oral briefings in advance of meetings of the relevant EU Council of Ministers to enable the Select Committee to make known its views: Provided that the Committee may also require such attendance following such meetings;

(6B) power to require that the Chairperson designate of a body or agency under the aegis of a Department shall, prior to his or her appointment, attend before the Select Committee to discuss his or her strategic priorities for the role;

(6C) power to require that a member of the Government or Minister of State who is officially responsible for the implementation of an Act shall attend before a Select Committee in relation to the consideration of a report under Standing Order 164A;

(7) subject to any constraints otherwise prescribed by law, power to require that principal office-holders in bodies in the State which are partly or wholly funded by the State or which are established or appointed by members of the Government or by the Oireachtas shall attend meetings of the Committee, as appropriate, to discuss issues for which they are officially responsible: Provided that such an office-holder may decline to attend for stated reasons given in writing to the Committee, which may report thereon to the Dáil;

(8) power to engage, subject to the consent of the Houses of the Oireachtas Commission, the services of persons with specialist or technical knowledge, to assist it or any of its sub-Committees in considering particular matters; and

(9) power to undertake travel, subject to—

(*a*) such recommendations as may be made by the Working Group of Committee Chairmen under DSO 108(2)(*a*) and SSO 104(2); and

(b) the consent of the Houses of the Oireachtas Commission, and normal accounting procedures.

(10) In accordance with Articles 6 and 8 of Protocol No. 2 to the Treaty on European Union and the Treaty on the Functioning of the European Union (Protocol on the Application of the Principles of Subsidiarity and Proportionality)

as applied by sections 7(3) and 7(4) of the European Union Act 2009, the Committee has the power to-

consider whether any act of an institution of the European Union infringes the principle of subsidiarity (DSO 116; SSO 109); and

form a reasoned opinion that a draft legislative act (within the meaning of Article 3 of the said Protocol) does not comply with the principle of subsidiarity (DSO 114 and SSO 107).

Appendix 3 – Witnesses and Official Report

14 June 2017:

- Officials from the Department of Justice and Equality; and
- Representatives from the Office of the Data Protection Commissioner ('DPC').

Official report

21 June 2017:

- Denis Kelleher, barrister-at-law.

Official report

5 July 2017:

- Representatives from Digital Rights Ireland ('DRI'); and
- Dr Geoffrey Shannon, Special Rapporteur on Child Protection.

Official report

Appendix 4: Opening statements

Pre-legislative scrutiny of Data Protection Bill

Opening statement

At the outset, I want to thank you, Chair, and the Joint Committee, for this opportunity to participate in the pre-legislative scrutiny of the General Scheme of the Data Protection Bill.

I am Seamus Carroll from the Civil Law Reform Division of the Department of Justice and Equality, and I am accompanied today by my colleagues Noreen Walsh and Conor O'Riordan from that Division.

Before entering into detail, I should perhaps outline briefly the background to the draft Bill.

Following four years of intensive negotiations, the JHA Council and the European Parliament reached agreement on updated EU data protection standards in December 2015. The texts of two new EU data protection instruments – firstly, a Regulation containing general data protection rules and, secondly, a Directive containing rules applicable to competent bodies involved in the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties – were published in May 2016. The Regulation enters into force on 25 May 2018; the Directive must also be transposed into national law by May 2018.

While the introduction of a single EU instrument containing all data protection rules would have been simpler and, possibly, more efficient, the European Commission decision to propose both a Regulation and a Directive was, despite some misgivings, accepted by the JHA Council and the European Parliament.

The introduction of new, higher EU data protection standards at this time can be justified for the following reasons:

- The inclusion of a new legal basis for data protection standards in Article 16 of the TFEU, together with the introduction of the right to data protection in Article 8 of the EU Charter of Fundamental Rights;

- The fact that existing data protection standards, which derive from the EU's 1995 Data Protection Directive and predate technological advances such as hand-held internet access and access to services, social networking and Big Data, as well as new business models such as cloud computing, are inadequate and ineffective to meet the challenges of the digital economy;

- The rapidly developing case law of the Court of Justice in relation to the protection of personal data;

- The need for more consistent interpretation and application of general data protection rules across the EU pointed towards the need for a more detailed, directly applicable Regulation rather than a Directive.

From the outset, Ireland supported the broad thrust of the European Commission's reform proposals, which sought to ensure that data protection rights and safeguards kept pace with developing technologies and new business models; otherwise, there would be insufficient citizen and consumer trust in the digital economy and its innovation, growth and jobs potential would not be realised.

Broadly speaking, both the Regulation and the Directive seek to strengthen individuals' data protection rights (data subjects), and to specify in more detail than at present the obligations placed on entities in the public and private sectors that process personal data (data controllers and data processors).

More concretely, both instruments place increased emphasis on the following:

- Transparency: the Regulation states that personal data must be processed lawfully, fairly and in a transparent manner; information must be provided to data subjects in a concise, intelligible and easily accessible form, using clear and plain language; the current access request fee of €6.35 will be abolished;

- Accountability: both the Regulation and Directive make it clear that data controllers shall be responsible for, and be able to demonstrate compliance with, data protection standards; data controllers must have detailed written arrangements with any data processors acting on their behalf;

- Security: personal data must be processed in a manner that ensures appropriate security standards, i.e. technical and organisational measures must be put in place to ensure a level of security appropriate to the risks involved. In future, all data breaches must be reported to the Data Protection Commission.

I will turn now to the General Scheme of the Data Protection Bill 2017.

As already mentioned, we are faced with a generally applicable Data Protection Regulation setting out data subject rights and data controller obligations with limited flexibility for the Member States, and a Directive that focuses specifically on the law enforcement and criminal justice area.

The broad objectives of the Bill, therefore, are as follows:

- To give 'further effect' in national law to the Regulation where permitted by the Regulation;

- To transpose the Directive into national law;
- To establish a Data Protection Commission to replace the Data Protection Commissioner and to equip that Commission with the mechanisms required to perform its tasks and exercise its powers in an effective manner.

Part 1

This contains a number of standard provisions. As regards repeal of existing data protection law as set out in the Data Protection Acts 1988 and 2003, the matter is still under consideration. While the Regulation and Directive will largely supersede these Acts, a potential difficulty arises from the fact that Article 2.2 of the Regulation specifies that its provisions do not apply to the processing of personal data in the course of an activity that falls outside the scope of EU law; recital 16 makes it clear that such activities include national security.

Part 2

The entry into force of the Regulation and this Bill, when drafted and enacted, in May 2018 will have significant implications for the workload of the Data Protection Commissioner. The workload is likely to increase, and investigations will become more complex, especially those with cross-border aspects. Both the Regulation and the Directive confer a broader range of tasks and powers – investigative powers, corrective powers, authorisation and advisory powers – on our Data Protection Commissioner.

In preparation for the coming into force of the Regulation and Directive in 2018, the resources of the Office of the Data Protection Commissioner have been increased to €7.526m for 2017, up from €1.9m in 2014. The additional funding has facilitated the recruitment of additional staff, including legal, technical and investigative experts. It is expected that the Office will have almost 100 staff members by the end of 2017. The issue of any further resource requirements for 2018 will be considered in the context of the Estimates process for 2018.

Part 2 contains proposals that will establish a Data Protection Commission to replace the Data Protection Commissioner. Head 9 provides that the Commission will consist of at least one member and not more than three members. This means that the appointment of additional Commissioners in response to an increased future workload will be possible without the need for amending legislation. To be clear, this does not represent an immediate change but will permit further appointments if needed in the future as a result of increasing workloads. Commissioners are required to have the qualifications, experience and skills needed to perform the duties and exercise the powers of the Commission.

The opportunity is also being taken to update the funding and financial control mechanisms applicable to the Commission in order to underpin the complete independence that the Commissioner already enjoys under current law.

The Regulation contains what has become known as a "One-Stop-Shop" mechanism that is intended to streamline the handling of alleged infringements of data protection standards across the EU. It is based on the concept of a "lead" supervisory authority, i.e. the Data Protection Authority of the Member State in which an entity's "main" establishment – or only establishment – within the EU is located. It means that where a data controller's main, or only, EU establishment is located in this jurisdiction, all complaints relating to that controller's data processing activities that are not exclusively local in nature must be investigated by the Data Protection Commission irrespective of the Member State of origin of the complaint. The Commission may request mutual assistance from the supervisory authorities of other Member States for investigation purposes; however, the decision as to whether or not an infringement has occurred, or is occurring, will, in the first instance at least, be that of the Commission.

Committee members will immediately appreciate the significance of this in light of the large number of international ICT companies with their EU headquarters located in this jurisdiction.

Before arriving at any final decision in such cross-border cases, the Commission will be required to submit a draft decision to the so-called "consistency mechanism"; in practice, this means that any proposed action arising from an investigation or enquiry must be circulated to other relevant supervisory authorities for their views. The Commission will then be required to have regard to any objections received from them and if there are any remaining objections to the proposed course of action, the Commission will be required to trigger referral of the case to the European Data Protection Board (EDPB) for further consideration. The EDPB, which will comprise of representatives of all supervisory authorities, will consider outstanding issues and may then take a binding decision by majority vote. Any binding decisions of the Board may be appealed to the Court of Justice in Luxembourg.

Part 3

The Data Protection Regulation is somewhat unusual insofar as it provides a certain margin of flexibility for Member State law, especially in respect of data processing activities undertaken by their public sectors. That gives rise to the need for implementing national law. This Part of the Bill seeks, therefore, to give further effect in national law to various Articles in the Regulation that allow a margin of flexibility. These include the following:

- Head 16 – blank for the present while awaiting a specific Government decision on the matter – which will provide for the digital age of consent. Article 8 of the Regulation requires the holder of parental authority to consent to the provision of information society services to a child under 17; however, Member States may provide by law for a lower age as long as it is no lower than 13 years. Following completion of a consultation process, it is expected that the Government will take a decision in respect of the age threshold that will apply in this jurisdiction in the coming weeks.

- Head 17 makes provision for the making of regulations permitting the processing of sensitive personal data for reasons of substantial public interest; a similar provision is found in Section 2B(1)(xi) of the 1988 Act (as amended).

- Head 19 makes provision for the processing of personal data relating to criminal convictions and offences for specified purposes; such processing must be subject to appropriate safeguards for the rights and freedoms of the individuals concerned.

- Head 20 provides for the making of regulations to restrict the exercise of data subject rights in order to safeguard important objectives of general public interest as permitted under Article 23 of the Regulation; this would , for example, be used to protect investigations of alleged professional misconduct or incompetence from access requests for the duration of the investigation. Any such restrictions must however respect the essence of the individual's fundamental rights and be a necessary and proportionate measure in a democratic society.

- Head 23 makes provision, exceptionally, for the possible imposition of administrative fines on public authorities and bodies when acting as undertakings; this will help to ensure fairness in cases in which both public and private bodies are providing similar goods and services.

- Head 24 seeks to give effect to Article 85 of the Regulation, which recognises that it is a matter for Member State law to reconcile the right to the protection of personal data with the right to freedom of expression and information, both of which are rights included in the EU Charter of Fundamental Rights. In recognition of potential conflicts between these rights in specific cases, subhead 3 will permit the Data Protection Commission to refer any question of law to the High Court for determination.

Before moving on, I should also say that the Regulation requires that all public authorities and bodies must designate a data protection officer (DPO). The DPO, who will act as a contact point for data subjects and the Data Protection Commission, must be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practice. He or she must be given the resources required to act in an effective and independent manner, free from conflicts of interest, and will report directly to the highest management level of the public authority or body concerned.

Part 4

This Part seeks to give effect to the Data Protection Directive. As outlined in Head 27, it 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.

"Competent body" is defined in Head 26 as:

(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.

It should be noted that certain public authorities and bodies will be subject to both the Regulation and the Directive depending on the processing concerned. In the case of a local authority, for example, routine data processing activities such as payroll, human resources, etc. will be subject to the rules of the Regulation, while data processing in the context of the prosecution of offences under the Fire Services Act will be subject to the Directive's rules. Similarly, prosecution activities of other bodies such as the Health and Safety Authority will fall under the Directive's rules.

Many of the data subject rights and data controller obligations in the Directive are broadly similar to those in the Regulation. However, as regards the former, the grounds for non-compliance with a data subject request for access to personal data, or for rectification, erasure or restriction of processing, which are set out in Head 37 are, as might be expected, more extensive. These provisions give effect to Articles 13.3, 15 and 16.4 of the Directive. However, where Head 37 applies, an individual may seek verification or review of the lawfulness of any processing by the Commission. The Commission will in due course inform the individual that verification or review has taken place and inform the individual concerned of his or her right to a judicial remedy.

In Chapter 3, Head 40 imposes a 'risk-based' approach on competent authorities; this means that each such authority must adopt and implement appropriate technical and organizational measures in order to ensure and be able to demonstrate compliance with the Directive's data protection standards. Obligations to carry out data protection impact assessments, report data breaches, engage in consultation with the Data Protection Commission and designate a DPO are also contained in this Chapter.

Chapter 4 contain provisions governing the transfer of personal data to Third Countries, while Chapter 5 makes provision for remedies, liability and penalties. In accordance with Article 56 of the Directive, Head 58 clarifies that a person who suffers material or non-material damage because of data processing that infringes data protection law may seek compensation for the

damage or distress suffered. This extension of liability to non-material damage under the Directive is significant and is broadly similar to that in Article 80 of the Regulation.

Chapter 6 contains provisions that specify the tasks and powers of the Data Protection Commission. In particular, Head 61 proposes to confer a range of corrective powers on the Commission.

Part 5

This Part contains provisions governing the exercise by the Data Protection Commission of its supervision and enforcement powers. Some powers are carried over from the current Acts (e.g. information and enforcement notices), while others are new (e.g. power to seek a High Court order to suspend or restrict data processing or data transfers to a Third Country; power to require submission of a report).

Both the Regulation and the Directive require that the exercise by supervisory authorities of their powers be subject to appropriate procedural safeguards, including judicial review and due process. The following safeguards, therefore, have been included in this Part:

- The investigative (Heads 74 to 76) and adjudicative (Head 77 to 78) functions of the Commission will be structured and managed separately; this is in line with Article 6 case law of the European Court of Human Rights;

- Provision is being made not only for appeals against administrative fines (Head 79), but for confirmation of fines by the Circuit Court in the event that they have not been appealed (Head 80). In the latter case, the role of the Court will be to confirm that due process has been observed.

Part 6

Without prejudice to the right to lodge a complaint with a supervisory authority, both the Regulation and the Directive require that data subjects have the right to an effective judicial remedy. Provision for this is made in Head 91. Recourse to the courts is necessary in any event in those cases in which a data subject claims compensation for material or non-material damage suffered as a result of a breach of data protection law. Head 90 makes provision for the appointment of a supervisory authority to supervise the processing activities of courts when acting in their judicial capacity. Article 8 of the Charter of Fundamental Rights provides that compliance with its rules shall be subject to control by an independent authority.

Before concluding, I should say that there have been extensive consultations with Government Departments, public authorities, representative bodies and the Data Protection Commissioner during preparation of the General Scheme of the Bill. However, I also want to say that a number of policy issues are still under review and consultations with the European Commission, the

Attorney General's Office and the Data Protection Commissioner are continuing. These relate to matters such as compensation claims, processing of conviction-related data and other sensitive data, and direct marketing activity by those seeking election to political office. Nevertheless, in view of the very tight timeframe in which we are working, it has been necessary to proceed with the General Scheme in advance of final resolution of these issues. The intention is to publish the Bill in the autumn, which will allow sufficient time for detailed consideration of its contents prior to enactment.

Conclusion

Implementation of updated EU data protection standards involves a complex interplay between the Data Protection Regulation which has direct effect but which allows, at the same time, a margin of flexibility for Member States, and a Directive which must be transposed into national law. The future decision-making role of the European Data Protection Board and the evolving case law of the Court of Justice will help ensure that data protection will remain an active and challenging area of law in the years ahead.

I hope that I have provided some clarity on the content of the Bill and the background to it. We are of course happy to respond to any questions that you may have.

Thank you for your attention.

Opening Statement of the Data Protection Commissioner

General Scheme of the Data Protection Bill 2017

14 June 2017

Introduction

1. As the Data Protection Commissioner (DPC), I would like to thank the Chairman and the members of the Committee for the invitation to attend today to discuss the provisions of the General Scheme of the Data Protection Bill 2017. In attendance with me are Deputy Commissioner John O'Dwyer who is Head of Investigations in my office, and Deputy Commissioner Anna Morgan who is Head of Legal in my office.

2. The DPC welcomes the early publication of the General Scheme of the Data Protection Bill 2017 which is intended to give effect to the General Data Protection Regulation (the GDPR) which will apply as an EU law on 25 May 2018.[1] The GDPR represents the most significant overhaul of EU data protection laws since 1995, when the existing Data Protection Directive (Directive 95/46/EC) came into effect. The GDPR states that upon it coming into force on 25 May 2018, the Data Protection Directive will be repealed.

Purpose and effect of the GDPR

3. Before I address the DPC's position in respect of specific issues concerning the General Scheme of the Data Protection Bill, it may be helpful to recall the essential purpose of data protection law as it currently stands, before going on to briefly outline the purpose and effect of the GDPR.

4. By 1995, it was already clear that developments in information technology had led to a dramatic increase in the volume of personal information being handled and processed by both public and private bodies. While some of that processing served useful and important social and/or economic needs, much of it was considered inappropriate, in the sense that individuals were losing control over who had access to their private information, and what use might be made of such information by third parties. Particular concern arose about the

[1] The Data Protection Bill will also transpose the Directive 2016/680 which deals with the protection of personal data in the context of processing by law enforcement authorities (the "**Law Enforcement Directive**"). Article 2.2(d) of the GDPR expressly states that the GDPR does not apply to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties. Instead, processing of personal data for these purposes are set out in the Law Enforcement Directive, which shares many points of commonality with the GDPR in relation to certain principles and rights of data subjects, albeit that these are subject to modifications to reflect the fact the purposes of such processing is concerned with law enforcement activities. The DPC will be the relevant supervisory authority responsible for monitoring the application of the Law Enforcement Directive. Separately, the EU also plans to adopt a new Regulation amending the law concerning data protection in electronic communications.

possibility that a person's private information might be used by third parties to make decisions impacting on them by means of automated processes, without that person even being aware of such processes or decisions, and perhaps without that person knowing what personal information the decision maker held about them, where they got it, or the purposes for which they held it and used it. Against that backdrop, data protection rules were developed, drawing from existing privacy law principles, e.g. the principle that a person should have control over when and in what circumstances their private correspondence might be scrutinised by a third party. In simple terms, then, the data protection rules aimed to give individuals control over their personal information, ensuring that they, and they alone, would decide whether, how and by whom that information might be used, and holding to account those parties who obtain and process such information.

5. Importantly, the rights of the individual to control how their personal data is used were significantly strengthened when data protection rights were recognised explicitly in the Lisbon Treaty[2] and in the Charter of Fundamental Rights[3] of the EU.

6. The GDPR represents a further milestone. It might be said to be designed to do three things:

    a. Because the EU's data protection rules were introduced by means of a *Directive*, the implementation of the rules became somewhat fragmented. By setting out the rules in a *Regulation*, the GDPR seeks to achieve effective harmonisation of the rules across the member states. (As the Chair and Committee members will be aware, an EU Regulation is binding in its entirety and is directly applicable in all EU member states without any requirement for national transposing legislation. In contrast, a Directive preserves a margin of flexibility to member states as to how to give effect to the principles set out in the text of that Directive. National legislation is typically required to transpose those principles into national law).

    b. Equally importantly, the GDPR is intended to modernise the laws on data protection in order to take account of technological developments, in particular the exponential reach of the digital and online environments and the risks which such advancements pose to the protection of individuals' personal data. One of the key objectives of the GDPR is to create a legal framework for processing personal data which fosters trust by individuals concerning the way in which their personal data is treated, thereby facilitating the development of the digital economy in the internal market and the free flow of personal data within the EU. As part of this, the GDPR introduces new rights for data subjects such as the right to data portability, the right to erasure and the right not to be subject to automated decision-making including profiling.

    c. Thirdly, and perhaps most importantly, the GDPR recognises that the rules contained in the Directive were not being implemented in a way that provided meaningful and effective protection for individuals. Too often, commitments set out on paper were not being delivered on in practice. As such, whilst the Directive set out to regulate those engaged in the processing of personal information, it did

[2] Article 16
[3] Article 8

not always enable such parties to be held to account in those cases where they failed to respect the rights of data subjects. With this in mind, the GDPR seeks to make more concrete the existing package of rights and protections enjoyed by data subjects. One of the key ways in which it does this is by introducing the principle of accountability. This principle means that data controllers must be able to demonstrate how they comply with the rules set out in the GDPR and, where they fail to do so, they will be held to account, e.g. by means of the imposition of administrative fines. Other notable areas of change include a tightening around the rules which apply to reliance on the consent of the data subject as a legal basis for processing and, equally, a restriction on the availability of the "legitimate interests" processing basis.

7. Finally, I would like to briefly refer to the very significant changes which the GDPR introduces in relation to the role and powers of data protection regulators in the EU, including the DPC. The GDPR establishes a significant range of investigatory, corrective, advisory and authorisation functions and powers for data protection supervisory authorities aimed at positioning supervisory authorities so that they can effectively monitor and ensure compliance with the rules for the protection of personal data and impose sanctions for infringements of these rules in the member states. The General Scheme seeks to give further effect to the exercise of these powers by the DPC, by way of for example Heads 66 to 70. However, by far the most publicised aspect of these powers and functions is the fact that that all EU data protection authorities will acquire administrative fining capability under the GDPR, with an obligation to impose sanctions that are effective, proportionate and dissuasive. The maximum administrative fine which may be levied under the GDPR is the greater of either €20 million or up to 4% of the total worldwide annual turnover for the previous financial year. As I have previously commented on this issue, the acquisition of an administrative fining capability is a game-changer in terms of the enhanced regulatory clout of the DPC under the GDPR.

8. The GDPR also calls for mandatory co-operation between the data protection authorities of member states in cases of cross-border data processing. One of the much talked about features of the GDPR is the requirement that data protection authorities co-operate with each other under the one stop shop mechanism in order to achieve EU wide consistency of approach in relation to the application of the GDPR. This one stop shop mechanism is aimed at making it easier for multinational companies to do business across Europe by being subject to just one regulator and their enforcement actions rather than being subject to multiple regulatory actions. The one stop shop hinges upon the idea of one lead supervisory authority being responsible for considering a complaint and reaching a draft decision where issues of cross border processing are involved but that authority has to take "utmost account" of the views of any other data protection authority who is deemed to be concerned with the cross border processing.

9. The GDPR sets out the principle that the lead supervisory authority will be the data protection authority in the member state where the organisation in question has its main establishment, in other words its place of central administration within the EU. Due to the large number of multinational corporates which are headquartered in Ireland, this means that the Irish DPC will be the lead supervisory authority in many cross-border cases which

will be dealt with by the one stop shop mechanism. That position will undoubtedly attract international interest in the DPC's handling of one stop shop cases. In anticipation of these developments, and with the support of Government, you will be aware that my Office has been gearing up by expanding the volume and range of the technical and personnel resources needed to carry out our expanded role.

Preparation of the General Scheme

10. As noted, the GDPR takes the form of a Regulation rather than a Directive and so, in principle, no implementation legislation is required to give effect to its key provisions. However, because some of the changes provided for under the GDPR are novel, some national legislation will be required to provide an effective framework for its implementation in practice. To take just one example, I have mentioned how, as part of its accountability agenda, the GDPR provides for the levying of administrative fines for infringements of the data protection rules. Such a mechanism gives rise to challenges under Irish law because, generally-speaking, our Constitution provides that only the Courts can impose penalties. To ensure compatibility with existing Constitutional law principles, legislation will be required to regulate the exercise of the new power conferred on my Office to levy administrative fines.

11. Before turning to address particular aspects of the General Scheme of the Data Protection Bill, I would like to acknowledge the huge amount of preparatory work which has been done by officials from the Department of Justice and Equality, in particular Seamus Carroll and Noreen Walsh, in drafting the General Scheme of the Data Protection Bill 2017. As the Chair and Members of the Committee will be aware, the General Scheme deals with multiple complex legal issues concerning not only issues of data protection law but it also has necessitated careful consideration of wider issues of European Union law, and Irish Constitutional and administrative legal principles, amongst other issues. The DPC is appreciative of the opportunities which have been extended to us over recent months to comment on the draft heads as they have been prepared by the Department officials and to contribute to informing the drafting process, including by sharing the DPC's practical experience of regulating in the area of data protection under the existing legislation. While there remains a large number of areas of the General Scheme which will need to be further developed during the formal legislative drafting process over the forthcoming months, we also acknowledge that considerable regard has been paid to date to the range of matters which the DPC has raised in the preparatory stages of the General Scheme.

12. However, from the DPC's perspective, there remains a number of fundamental issues arising from the General Scheme which give cause for real concern because of their potential impact on the regulatory environment and the ability of my Office to effectively exercise our supervisory and enforcement powers under the GDPR as currently contemplated by the General Scheme. Three issues are examined below. These are:

    a. **The question as to whether our existing data protection legislation is to be repealed or retained;**

b. The application of administrative fines procedures to public bodies and authorities; and

c. The handling of complaints under the GDPR.

Retention of portions of the existing legislation

13. As noted above, it is intended that, when the GDPR comes into effect in May 2018, the existing EU Directive 95/46/EC will be repealed in its entirety, reflecting the fact that the GDPR is intended to represent a "clean-slate", establishing a single legal instrument in which data protection rules and principles will be set out.[4]

14. Against this backdrop, the primary and overarching concern of the DPC relating to the General Scheme is the fact that, unlike the position that will apply at EU level, there is no commitment to repealing the entirety of our existing national legislation – the Data Protection Acts 1988 and 2003. Head 5 of the General Scheme states that *"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 therefore appears that, as yet unidentified portions of those Acts may be retained while other, as yet unidentified provisions, may be repealed. The DPC disagrees with any proposal to retain, even in part, the Data Protection Acts 1988 and 2003 and strongly favours the complete repeal and replacement of the existing legislation with a new omnibus Data Protection Act. There are a number of reasons for the DPC's position in this regard, which I would like to outline in brief for the benefit of the Chair and the Members.

(i) Accessibility and legal certainty

15. The first ground for the DPC's objection to retaining part of the existing data protection legislation relates to the accessibility, and how understandable, the resulting legislative framework would be. The DPC strongly holds the view that the more complicated a piece of legislation is, the less likely it is to be fully understood by the stakeholders to whom it is addressed, resulting in diminished compliance levels. For this reason, and given the greatly enhanced obligations on data controllers and processors under the GDPR, it is critical that the GDPR is given effect in the State by way of legislation that is clear, certain and free from ambiguities. The DPC does not believe that this will be achieved by retaining parts of the existing legislation and over-layering them with new legislative provisions in the Data Protection Bill, as this will cause confusion and interpretative difficulties.

16. Recital 8 of the GDPR makes it clear that elements of the GDPR can only be incorporated into national law as far as is necessary for coherence and making the national provisions comprehensible to the persons to whom they apply. This means that the new Data Protection Bill can only contain supplementary provisions to the GDPR and cannot repeat what has already been stated in it. At a practical level, a person seeking to understand what the post-GDPR Irish data protection framework is, will have to start with text of the

[4] As noted earlier, however, data protection rules now derive, ultimately, from the EU Treaties and from the EU's Charter of Fundamental Rights.

GDPR in front of them and read that alongside the new national legislation. However, if some portions of the Data Protection Acts 1988 and 2003 are retained, and other parts are repealed, this means that a person seeking to understand the data protection legislative regime in Ireland will have to establish which of these "old" provisions are still in force and then read them alongside the GDPR and new Data Protection Act. As such, all stakeholders would have to try to weave their way through a dense legislative maze of three separate legislative sources (the remnants of the Data Protection Acts 1988 and 2003, the GDPR and the new Data Protection Act) in order to try to understand their respective rights and obligations. Furthermore, insofar as electronic communications are concerned, the forthcoming EU Regulation on data protection in the electronic privacy context (which is still making its way through the EU legislative process) would also have to be consulted as a fourth relevant legislative text.

(ii) A new era in data protection law & reputational consequences

17. The retention of portions of existing legislation is not consistent with the EU policy objective of a new modernised data protection regime heralded by the GDPR, which, as I mentioned above, is intended to be a harmonised law reflective of the digital age and consistent with the EU Digital Single Market agenda. A patchwork legislative framework consisting of statutory provisions which are (in the case of the 1988 Data Protection Act) 29 years old, combined with updated statutory provisions (designed to take account of the digital revolution) could be perceived as a lack of commitment to the new data protection regime in the EU and could be damaging for the State's and the DPC's reputation.

(iii) Ireland as a lead supervisory authority

18. As I have previously mentioned, under the GDPR, the DPC will assume the role of "lead supervisory authority" for a large number of multinational companies that have their European headquarters in Ireland. The DPC believes that the existing international focus on the DPC, as one of the most important data protection regulators in Europe, will only increase post-GDPR. There will inevitably be a huge amount of scrutiny as to the domestic measures taken by the State to give effect to the GDPR. This makes it all the more critical that Ireland's domestic legislative framework is as simple and accessible as possible so that Ireland is perceived as having, and actually has, a robust but accessible legislative framework which is appropriate to the critical role which the DPC will perform as a lead supervisory authority under GDPR. The message that the Government has been sending out globally is that Ireland will be "best in class", leading the way in best practice in European data protection regulation but the DPC's position is that this aim would be greatly undermined by the retention of parts of the pre-GDPR legislative regime.

19. The DPC understands from Head 5 of the General Scheme that the reason why parts of the existing legislation may be retained is to ensure that Ireland continues to meet its obligations under the Council of Europe Convention on data protection[5] (known as Convention 108). That convention was implemented in Irish law by means of the Data Protection Act, 1988. The concern, therefore, is that, if our existing Data Protection Acts

[5] Convention for the protection of individuals with regard to automatic processing of personal data 1981

are repealed, some elements of Convention 108 may also fall away, putting Ireland in breach of its commitment to implement the convention in full.

20. While the DPC accepts that this is a valid concern, it is relevant to note, however, that all 28 member states of the EU have ratified Convention 108 and will therefore also have to deal with the same issue. The DPC therefore urges that a solution be identified, whether at a national level or in conjunction with the EU Commission, which would allow the complete repeal of the Data Protection Acts 1988 and 2003 so that the new Data Protection Bill is enacted as a complete and standalone law. This is critical to avoid the potentially serious consequences which I have identified which would likely flow from retaining parts of the existing legislation.

Administrative fines for public authorities and bodies

21. Another serious matter of concern for the DPC under the General Scheme relates to Head 23 and the imposition of administrative fines on public bodies and authorities. The GDPR states in Article 83 that it is for each member state to lay down the rules on whether, and the extent to which, public authorities and bodies can be subject to administrative fines. Head 23 of the General Scheme provides for public bodies and authorities to be subject to administrative fines in a limited way only, i.e. they would only be subject to administrative fines where they are engaged in commercial activity as an "undertaking", as defined under Section 3 of the Competition Act 2002. In essence, and as illustrated by the explanatory notes to this Head, this would mean that public bodies could be fined only where they are providing goods or services in the same market as private companies, the rationale being that not imposing fines in such circumstances could cause competition distortions. However, the DPC's firm position is that all organisations should be treated in the same way without distinction as to whether they are engaged in commercial activity or any other activity, so that, in principle, all public bodies and authorities are capable of being fined where they infringe the GDPR. If this is not the case, the deterrent value of administrative fines in the public sector would be nullified. Based on its experience in regulating the public sector to date, the DPC's position is that making all public authorities/ bodies liable to administrative fines is crucial if we are to encourage greater levels of compliance with data protection law amongst public authorities and public bodies than that sector has traditionally demonstrated.

Handling of complaints under the GDPR

22. The final issue which I would like to bring to the attention of the Chairman and Members of the Committee relates to the changes which the GDPR brings in, relating to the manner in which the DPC must deal with complaints from individuals concerning alleged infringements of their data protection rights. Under the Data Protection Acts 1988 and 2003, an individual has the statutory right to seek a decision from the DPC in all cases where a complaint has been made to the DPC about a data controller or processor and that complaint cannot be amicably resolved. The GDPR takes a broader approach, envisaging outcomes to complaints other than decisions, e.g. the provision of guidance or information to the individual complainant in relation to resolving the issue with the data

controller or data processor. Reflecting this approach, the GDPR provides that an individual has the right to *lodge a complaint* with the relevant supervisory authority under Article 77, to have their complaint *handled,* and to be *informed within 3 months* on the progress or outcome of their complaint. It is also important to note in this context that the supervisory authority is required to investigate a complaint *"to the extent appropriate".*

23. Consistent with the intention of the GDPR that a supervisory authority will have a discretion as to the extent to which it investigates a complaint from an individual, the DPC's position is that it should be permitted to take a risk-based approach to investigations so that its investigatory resources and powers are most effectively and most appropriately utilised, for example in cases where systemic issues have been identified, or where the alleged infringements potentially affect (and therefore pose serious risks to the rights of) large numbers of individuals. The DPC is of course very mindful of its responsibilities under the GDPR to handle complaints from individuals and to investigate those individual complaints the extent appropriate. In this regard, the DPC is of the view that there is significant work still to be done during the legislative drafting process to identify and establish in the bill (or otherwise) the most appropriate, effective and efficient methods which can be deployed by the DPC in handling individual complaints, so as to facilitate individuals to vindicate their rights in the most effective manner.

24. For completeness, I would also note that data subjects will continue to enjoy a number of other protections in relation to complaints. For example, while the DPC will not be permitted to award damages or compensation, the GDPR confers a right on data subjects to apply to the Courts for an order directing a data controller or processor to pay compensation where the individual has suffered either material or non-material damage as a result of an infringement of the GDPR. It is clear from the GDPR that the right to compensation is not dependent upon, or connected to, any investigation by or actions taken by the supervisory authority. This right is provided for in Head 91 of the General Scheme under which both the Circuit Court and High Court have concurrent jurisdiction to hear and determine data protection actions brought by individuals.

25. I would like to thank the Chairman and the Members of the Committee for their attention and to invite any questions which the Chairman and the Members may have for my colleagues and I.

Dr DENIS KELLEHER BCL, BL

To Joint Committee on Justice and Equality

From Dr Denis Kelleher BCL, BL

Date 20th June 2017

RE **Submissions on Heads of Data Protection Bill 2017**

The introduction of the *Data Protection Bill 2017* to the Oireachtas will begin a process by which data protection law will become increasingly central to Irish law, public administration, commercial activity and the day-to-day lives of Irish people. That law will inevitably become more complex as a result. At present we have a single set of data protection rules set out in the *Data Protection Acts 1988 and 2003* ("DPA"). From May of next year we will have at least three sets of rules:

- The overarching EU General Data Protection Regulation or GDPR;
- The new *Police and Criminal Justice Authorities Directive (2016/680)* , which applies to the processing of personal data in the criminal justice sector. This will be implemented by the *Data Protection Bill 2017;* and
- A residual set of Irish rules that will cover domestic matters falling outside the scope of EU law, my understanding is that these rules will primarily cover national security.

Other sources of law will add to this complexity over the coming years. In addition to the above we will also have:

- The new ePrivacy Regulation, a draft of which is being considered by the EU Commission;
- Other EU rules, which are already being made such as the second Payment Services Directive;
- Rules under Article 39 of the Treaty on the European Union, which will deal with the processing for foreign and security policy; and,
- Judgments of the Court of Justice of the EU, which is increasingly redefining EU data protection rules in judgments such as *Mac Fadden*, *Breyer* and *Tele 2 Sverige*

The publication of these Heads marks a first step in this process. These Heads reflect the hard work and expertise that the team in the Department of Justice have applied to the difficult job of analysing how the GDPR may be adapted to Irish law and how the new Data Protection Directive may be implemented. The length and complexity of the Heads reflects the difficulty of this task. It would be impractical for me to provide an analysis of the Heads in their entirety. Instead my submission focuses on the following issues:

1. The role of the Data Protection Commissioner;
2. Should the existing Data Protection Acts be repealed and replaced or amended?
3. The role of identification services under the GDPR;
4. The role of the Oireachtas under the GDPR; and,
5. Damages.

denis@ictlaw.com
00 353 87 2322409

1. The role of the Data Protection Commission

The Bill proposes that the existing Data Protection Commissioner be replaced with a three member Commission. This Data Protection Commission is required to be independent by the EU Treaties and the GDPR itself. It is important to realise that the existing Data Protection Commissioner (DPC) is fully independent. The EU Commission has successfully prosecuted three Member States (Austria, Germany and Hungary) before the EU's Court of Justice for failing to adequately ensure the independence of their Data Protection Authority. These prosecutions suggest that the EU Commission is vigilantly policing this independence. However, the EU Commission has not commenced any such prosecution against Ireland, which it suggests that our own DPC is properly independent under EU law. I have undertaken my own analysis and concluded that the DPC's independence is adequately protected under Irish law[1].

That said the Heads reflect Irish drafting conventions. Such conventions may give the erroneous impression that the Data Protection Commission is not fully independent. An example of this is Head 10.

Head 10 – staff of the Data Protection Commission

Head 10(4) provides that the Minister "may" delegate his functions under the Civil Service Acts to the Data Protection Commission. Given the over-arching EU Treaty obligation this is effectively an obligation, however the use of the word "may" is open to being misconstrued. I therefore suggest that this be changed to "shall".

Delegation of the Minister's functions under the Civil Service to the Data Protection Commission should be sufficient to ensure independence. However, it is worth noting that section 5(1) of the Civil Service Act 1957 (as amended by the *Civil Service Regulation (Amendment) Act 2005*) provides

> "Every established civil servant shall hold office at the will and pleasure of the Government"

The reality is that civil servants cannot be dismissed at will by the Government, or anyone else. However, provisions such as the above may give rise to the erroneous perception that the independence of the Data Protection Commission has in some way been compromised. There may be no need to create a new relationship between the Data Protection Commission and its staff; in general, the Civil Service Acts will be sufficient. Instead it may be useful if this Bill were to contain a general statement that staff of the Data Protection Commission are responsible only to the Data Protection Commission, even though such a provision simply repeats what the existing law already provides. Such a statement may be legally unnecessary and so contrary to best drafting practice, but it might be wise to include such a statement from a policy perspective.

Once these Heads are drafted as provisions of the Bill then a detailed analysis will have to be undertaken; the starting point for this analysis would have to be the operational needs of the Data Protection Commission. The purpose of this analysis would be to ensure that the Bill matches how the Data Protection Commission actually anticipates it will work under the GDPR. I would make the following suggestions at this stage.

Delegation of Data Protection Commission functions

[1] Kelleher, *Privacy and Data Protection Law in Ireland,* Bloomsbury Professional, 2nd Ed., 2015, para 14.31-38, pp353-355.

denis@ictlaw.com
00 353 87 2322409

The Heads provide for the delegation of functions to the individual commissioners or members of staff in Heads 5(4) and (5). This would allow the Data Protection Commission to delegate the investigation of a complaint to one Commissioner and the making of a decision on that complaint to another. This may avoid the operation of the Data Protection Commission becoming unwieldy. It might also avoid an appearance of bias, which might be given if the Commissioner who undertook an investigation were to take a decision on the outcome of that investigation. A precedent for such a provision may be found at section 18F of the Central Bank Act 1942. It might also be worthwhile considering whether the Data Protection Commission should be able to appoint committees to manage certain functions such as HR or other operational issues. A precedent for this function might be found at section 18D of the Central Bank Act 1942.

Head 7 – Data Protection Commission

There may be no need to provide for the seal of the Data Protection Commission. A seal is highly relevant to a Minister, who will act in a personal and a political capacity. Where a seal is used there is a presumption that the Minister is acting in his official capacity. In contrast the Data Protection Commission will only operate in its official capacity, it does not have non-official functions. Hence I am not sure that there are any practical benefits to a seal, which comes with its own bureaucracy: it has to be kept in a safe and so forth. I would suggest that this provision might usefully be deleted.

Head 14 – Prohibition on unauthorised disclosure of information

These provisions are well designed; the reliance on the law of tort seems sensible, given the difficulty of prosecuting offences. However it only addresses the Data Protection Commission's own obligations. Some consideration might be given to the obligation that other public bodies may be subject and, in particular, whether "gateways" need to be provided to enable information to be transferred between the Data Protection Commission and other public bodies.

Head 23 - Imposition of fines on public authorities

Public authorities are subject to a different incentives to private sector entities. Fines may not be a particularly effective deterrent against bodies that draw from public funds. Any fines that are imposed by the Data Protection Commission will be paid to the State. Where the Data Protection Commission imposes fines on public bodies that are funded by the State then such fines may amount to no more than an accounting exercise. Monies that were originally paid out of State funds being refunded to the State, from where they may well be repaid back to the public body in question in order to ensure that public services are maintained. Hence the imposition of fines on public bodies may amount to no more than an accounting exercise.

Other deterrents against public bodies may prove more effective. I do not think that a public body may be any more or less susceptible to embarrassment or reputational damage than a private company. However if a public body is found to have been processing data illegally, i.e. in breach of data protection law, then previous decisions made by that body may be invalidated and future decisions cannot be made on the basis of the illegally processed information. This may then lead to claims for damages being brought against that public body. Where such claims are successful then damages will have to be paid out of, but not into, public funds.

denis@ictlaw.com
00 353 87 2322409

Head 90 – Supervisory authority for courts acting in judicial capacity

Some consideration needs to be given as to how a judge will act as supervisor for the Courts. As drafted the Bill suggests that investigator powers such as the power to appoint authorised officers are reserved to the Data Protection Commission alone. The Heads will need to address how the appointed judge will undertake such an investigation. Presumably it would be undertaken in cooperation with the Data Protection Commission, but this would need to be stated by the Heads. A judge acting in their supervisory capacity under this Bill and the GDPR will not be acting as a judge in their judicial capacity. Further detail may therefore need to be provided in relation to the functioning of the judge in that role.

2. *Should the existing Act be repealed?*

Ireland's data protection laws will be spread across a number of different Acts from May 2018. As noted above there is a single enactment at present but from May 2018 there will be three separate regimes:

- The General regime, which is set out in the GDPR itself, together with the adaptations made by this Bill;
- The criminal justice regime, which will be implemented by this Bill;
- The residual regime, for data processing operations that fall outside the scope of the above.

It is generally accepted that the first two of the above are necessary. However the last of these has proven more controversial. One difficulty is that it is hard to understand what, if any, data processing operations might fall within the scope of the residual regime. Charities might, but only if they limit their collections and donations to archaic systems. The processing of personal data for the purposes of national security would seem to fall within this residual regime. I would suggest the Oireachtas might want to carefully consider what controls it would wish to see in place where personal data is being processed for this process. Whether the Oireachtas would be able to give this consideration whilst simultaneously considering this Bill is a matter for the Oireachtas itself. I do agree with the DPC that:

> "…a patchwork presentation of the new Irish law in the form of a 2018 amendment Act rather than a completely new stand-alone Act does not create the impression of a new, modernised regime"

The difficulty is that repealing the existing Acts and re-enacting replacement provisions will take up Oireachtas time. This is time which the Oireachtas might better spend considering how GDPR should apply and the new Data Protection Directive 2016/680 should be implemented. As the Data Protection Commissioner has said, an incorrect impression will be given if this Bill amends an Act that will only apply to some residual activities. Ideally the old Acts would be repealed, but if that is not possible, then might the "optics" be addressed through the drafting process.

3. *The role of the State in supplying identification services*

The application of the GDPR will force the State to make a decision about the provision of identification services. Articles 8 and 22 GDPR require that suppliers of information society services verify the identity of data subjects so that they may distinguish between children and adults. The question of how that verification will be made then arises. The default option is that such verification services will be provided by the market. Alternatively, the State would

provide such services. The Oireachtas needs to decide which option it prefers. It could adopt the Estonian approach or it could do nothing. If the Oireachtas does nothing then the default option will apply. Hence, the Oireachtas will make a decision on this matter one way or another.

My own preference is that it would not be necessary to use such identification services at all. However, the reality is that from May 2018 providers of some information society services will have to be able to verify my age and identity. I would far prefer that my identity be verified by the State, not the private sector, but the State must provide such services if I am to use them.

4. The role of the Oireachtas under the GDPR

The GDPR will change the role of the Oireachtas in deciding how and when personal data is to be processed by the State. Article 36(4) GDPR provides:

> "Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing"

Recital 96 GDPR explains that this should be done "…in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject" This seems to mean that the Data Protection Commission would be consulted at this pre-legislative state of the process. Any concerns expressed by the Data Protection Commission might either be dealt with at this point, or else considered by the legislature during the legislative process itself. Head 46(8) makes general provision for this consultation to take place; you might want to consider whether some further detail should be included in the actual Bill.

In my view the GDPR may significantly increase the role of the Oireachtas in deciding how and when the State is to process personal data. There is a rather technical debate underway in relation to the extent to which legislation must be in place before personal data is controller or processed by the State. (I have made separate submissions to the Joint Committee on Finance, Public Expenditure and Reform, and Taoiseach on this point) Whatever the outcome of this debate may be, it is clear that the State will face significant consequences if it should process personal data without an adequate legal basis. These consequences may come in the form of failed prosecutions, failed delivery of programmes or significant claims for damages. Article 6(2) GDPR provides that Member States may:

> "…introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing…"

It may be that some such amendments will be brought forward in this Bill. In any event I would think it wise to anticipate that there will be many such amendments in future. The State is subject to the same obligations of Data Protection by Design and Default as is any other data controller. The State needs to clearly think-out how it intends to process personal data, then build systems that are designed to comply with the relevant data protection laws.

5. Damages

Article 82 GDPR provides:

> "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered"

I am aware that the German equivalent of this Bill provides for the award of compensation to persons and the issue has been raised of whether an equivalent provision is necessary here. I would have to say that my initial reaction was that it was not. I am not sure that there is a real distinction to be made between "the right to receive compensation" and "the right to compensation". If anything the former seems clearer than the latter. But the view may be taken that some national implementing measures are necessary. I would not see there being much

Of more significance may be Article 80 GDPR which provides that:

> "The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law"

This seems to effectively provide for class actions "where provided for by Member State law". The Irish Rules of Court do not provide for such class actions at the present time, though it does provide for representative actions. Class actions have the potential to be particularly significant for data protection as computers will process the personal data of large numbers of people in precisely the same way. If the computer gets it wrong in relation to one, then it will get it wrong in relation to all. And compensation may prove to be one of the most potent mechanisms by which subjects will assert their rights against controllers and processors. The operation of this mechanism will be determined by Rules of Court. Hence I would suggest that the Committee pay some attention to Head 92, which I think may prove to be one of the more significant provisions in this Bill.

Denis Kelleher **20th June 2017**

denis@ictlaw.com
00 353 87 2322409

Speaking Notes
Oireachtas Joint Committee on Justice and Equality
Pre-Legislative Scrutiny of Heads of Data Protection Bill 2017

Thank you to the Committee for the invitation to address you on the proposed Heads of Bill.

We should say at the outset that we think that the General Data Protection Regulation (GPR) presents a watershed in protection of citizens' rights. I intend to address three main areas, of the Heads of Bill, which I hope will be of assistance to the committee in their deliberations.

1. The proposal to exempt State agencies from administrative fines (Head 23).
2. Giving the required effect to the GDPR's requirement that there shall be a right to compensation for financial and non-financial loss arising from a breach of the Regulation (Head 91)
3. A proposal that the GDPR and Directive 2016/680 should be dealt with in separate legal instruments. The GDPR should be given full effect in a single Act, repealing and replacing previous legislation in this area.

1. Head 23

1.1. Head 23 of the General Scheme of the Data Protection Bill provides for administrative fines being imposed on public authorities or bodies solely in respect of their activities as an 'undertaking' .

1.2. This has the effect of exempting public authorities or bodies in respect of all activities where they are not acting as an 'undertaking'. This is a very unsatisfactory state of affairs from the point of view of good administration and of clarity of the law.

1.3. It is good administrative practice to allow for accountability for breaches of citizens' Fundamental Rights of Data Privacy. The most effective form of accountability is the risk of financial penalties on non-compliant organisations.

1.4. Administrative fines for public authorities or bodies are largely cost-neutral for the exchequer as a whole, as the central fund is the recipient of the fines levied.

1.5. The proposal as it is currently drafted introduces the legally complex test of whether a public authority is acting in the capacity of an 'undertaking', which will have to be completed by the Data Protection Commission every time it wishes to assess whether administrative fines may or may not be levied.

1.6. As the explanatory notes demonstrate, through using the examples of Medicall Ambulance Service Ltd –v- HSE and Lifeline Ambulance Services Ltd –v- HSE, this would likely be a contentious decision, open to challenge each time by the public body or authority.

Recommendation

1.7. It would be better if Article 83.7 was implemented without any restrictions on the administrative responses available to the Data Protection Commissioner, including such fines as the Commission found appropriate to breaches of citizens' personal data privacy.

2. Head 91

2.1. It appears that Head 91 is intended to give effect to Article 82 of the Regulation, as well as Article 56 of the Directive.

2.2. Article 82 GDPR says that Member States "shall' (future tense) make provision for recovery of compensation for both material and non-material damages.

2.3. The Heads of Bill recognises that there is a right of action, but not explicitly a right of compensation, by a data subject for breach of their rights.

Recommendation

2.4. It would be better to see the intent of Article 82 of the Regulation and Article 56 of the Directive being made explicit by way of an explicit legislative recognition of the right of recovery of compensation for both material and non-material damages.

3. Separate Implementation of Regulation and Directive

3.1. There is a compelling public policy argument that the law should be stated as clearly and in as accessible a manner as possible.

3.2. The Current General Scheme of the Data Protection Bill seeks to
(a) largely, but not completely, replace the existing Data Protection Acts. (Head 5)
(b) legislate for a small number of matters in the GDPR which have been left to member states.
(c) transpose entirely Directive 216/680 of the European Union (Primarily by way of Part 4 of the Heads of Bill).

3.3. Attempting to address these diverse and unrelated intents through a single piece of legislation runs the risk of failing to provide an optimum outcome for any of them.

Recommendation

3.4. It would be better to address the transposition of Directive 216/680 by way of a specific legislative instrument. This would allow any of the necessary residual elements required from the Data Protection Acts for that transposition to be restated.

3.5. This would then allow for the full repeal of the existing Data Protection Acts (currently intended for partial repeal under Head 5) and their replacement by the GDPR verbatim in Irish law, together with the small number of domestic legislative variations.

3.6. As well as providing clarity, this approach would significantly reduce the risk of legislative uncertainty and the likelihood of challenges to interpretation by the proposed new Data Protection Commission before the courts.

Joint Committee on Justice and Equality, Wednesday 5 July 2017

Comments on the General Scheme of Data Protection Bill (May 2017 draft)

Dr TJ McIntyre

Lecturer in UCD Sutherland School of Law, Chair of Digital Rights Ireland and Consultant with FP Logue Solicitors

Introduction

Digital Rights Ireland (DRI) is grateful to the Committee for the opportunity to make submissions in relation to the Heads of Bill. DRI is the only Irish civil liberties group focusing on issues of technology and fundamental rights and has extensive experience in the area of privacy and data protection. DRI was the lead plaintiff in the judgment of the European Court of Justice in *Digital Rights Ireland and Seitlinger and Others*[1] which invalidated the Data Retention Directive, was an *amicus curiae* in *Schrems*[2], which found the Safe Harbor decision on data transfers to the United States to be invalid, and was an *amicus curiae* in *Microsoft v. United States*[3], which prohibited extraterritorial access by the US Government to emails stored in Ireland. DRI continues to bring litigation in this area, including an ongoing High Court challenge to Irish data retention laws.

Structure of the Bill

Head 5 states that:

> 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.

DRI shares the concerns expressed in previous testimony by the Data Protection Commissioner and Dr. Denis Kelleher that retaining portions of the earlier acts will result in a complicated and confusing patchwork of laws in this area. If the earlier acts are not repealed, researching some issues (particularly at the boundaries between public and private processing of data) will require piecing together the GDPR itself, the 1988, 2003 and 2018 Acts, as well as any relevant statutory instruments. This is entirely at odds with making the law accessible to the public.

---

[1] Joined Cases C-293/12 and C-594/12.

[2] Case C-362/14.

[3] No. 14-2985 (2d Cir. 2016.

While there are still a number of areas covered by Convention 108[4] which fall outside the scope of the GDPR – in particular, as Convention 108 applies to automated personal data files in the public sector generally[5] – these areas are now considerably reduced as compared to the previous position under the Data Protection Directive and will require less work to identify and provide for. This is something which will have to take place in the relatively near future in any event, as the process for modernising Convention 108 (including aligning it to the GDPR) nears its conclusion.

DRI **recommends** that the 1988 and 2003 Acts be repealed, with those issues falling outside the scope of the GDPR included in a new, standalone, bill to parallel, as far as possible, the GDPR. This repeal and re-enactment should not undermine the additional rights provided for by those acts.

DRI also **recommends** that consideration be given to carving out Part 4 of the Bill[6] and enacting it as a standalone bill. As a practical matter, including Part 4 in the Bill is likely to lead to confusion between the similar but distinct systems which will apply under the GDPR and the Law Enforcement Data Protection Directive. Readers without a legal background may be confused by the many sections which might appear to implement the GDPR, but in fact are limited to the law enforcement context. Indeed, this may even trip up readers with a legal background. For example, Head 20 provides for "national security" restrictions to be made by ministerial regulation (in the context of the GDPR); however "national security" is defined only in Head 26 (in the context of the Directive) – inviting blurring of the boundaries between the two parts. Treating Part 4 as a separate bill would help to clarify the scope of these provisions.

Representation of Data Subjects

Article 80 GDPR provides for data subjects to be assisted in enforcing their rights by not-for-profit bodies. To explain why this is necessary, it may be helpful to refer to recently published research which examines how data protection law has been undermined by practices making it impossible for the average citizen to enforce their rights.[7] For example, in relation to subject access requests it found that:

---

[4] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Reference, ETS No.108.

[5] Article 3(1). Ireland has excluded certain personal data from the scope of Convention 108, as follows:
"[T]he Convention will not apply to the following categories of automated personal data files, which are set out at Section 1(4) of the Data Protection Act 1988, to wit :
a. personal data that in the opinion of the Minister for Justice or the Minister for Defence are, or at any time, were, kept for the purpose of safeguarding the security of the State ;
b. personal data consisting of information that the person keeping the data is required by law to make available to the public ;
c. personal data kept by an individual and concerned only with the management of his personal, family or household affairs or kept by an individual only for recreational purposes." (Declaration made at the time of deposit of the instrument of ratification, on 25 April 1990).

[6] Transposing the Law Enforcement Data Protection Directive, Directive 2016/680.

[7] Clive Norris and Xavier L'Hoiry, "Conclusion: The Law-in-Books, the Law-in-Action, and the Promise of Regulatory Reform" in Clive Norris et al., *The Unaccountable State of Surveillance: Exercising Access Rights in Europe* (Springer, 2016).

> To exercise their rights, citizens are faced with an obstacle course: just to get to the starting line they need to traverse a number of hurdles before they can exercise their rights, many fall at the first hurdle because they cannot even locate the legal entity to whom they must make the request. Some fall at the second hurdle, when they are authoritatively, but incorrectly, told that they do not have the right. Those who manage to proceed may still give up before the next, as they are worn out by delays and administrative inefficiencies. But even those who make it to the starting line and successfully manage to submit a subject access request, are still unlikely to know what data is collected about them, with whom it is shared and how it is processed... the whole range of informal practices, situational understanding, and non-legal norms come in to play to systematically discourage and thwart data subjects in successfully gaining access to their data and information about how it is processed and shared.[8]

Article 80 GDPR helps to remedy this power imbalance by permitting qualified not-for-profit bodies (such as consumer rights organisations, civil rights groups, or trade unions) to act on behalf of the data subject. It provides that:

> 1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77 [*right to lodge a complaint*], 78 [*right to an effective judicial remedy against a supervisory authority*] and 79 [*right to an effective judicial remedy against a controller or processor*] on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.
>
> 2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

To summarise, Article 80 has mandatory and discretionary parts:

- Member States must give effect to the data subject's right to mandate a non-profit to lodge complaints with a data protection authority and seek a judicial remedy (such as an order that data be destroyed) against a controller or processor.

- Member States may provide that a non-profit can seek compensation (damages) on behalf of a data subject.

---

[8] Ibid., 480.

- Member States may provide that a non-profit can, of its own accord, lodge a complaint with a data protection authority and seek a judicial remedy (such as an order that data be destroyed) against a controller or processor.

These Heads of Bill, however, fail to give effect to either of these two discretionary parts of Article 80, without any explanation as to why this narrow approach was chosen. This will both undermine fundamental rights and lead to practical problems. In particular:

- The ability of non-profits to assist individuals by bringing claims on their behalf is hampered by the fact that non-profits will not be able to seek compensation for those individuals. This creates a perverse incentive – those who are most harmed by an illegal practice will be the least able to ask a non-profit to bring an action on their behalf, as by doing so they will not be able to receive compensation. Instead they will have to bring a claim themselves, if they have the knowledge to do so, can afford to do so and can risk the legal costs involved.

- A knock-on effect is that this will lead to an increased number of cases before the courts, in a way which will be unmanageable for any large scale data protection breaches given the lack of any general provision for class-actions in Irish law.

- The failure to allow non-profits to bring complaints of their own accord means that illegal practices will go unchallenged unless a particular victim is identified and willing to step forward. This is a particular problem in areas of sensitive personal data where a complaint may be embarrassing, humiliating or even dangerous.

The need for non-profits to be able to bring complaints of their own accord has been recognised in our own litigation. In *Digital Rights Ireland Ltd v. The Minister for Communication, Marine and Natural Resources & Ors.*[9] the High Court granted *locus standi* to DRI to challenge data retention laws on behalf of the wider population on the basis that the privacy interests affected by those laws were "of great importance to the public at large" and without a representative action "it is unlikely that any given mobile communications user... would bring the case, given the costs that would be associated with any such challenge". It is unfortunate that this point has been ignored in the drafting of the Heads of Bill.

DRI **recommends** that the Heads of Bill be amended to provide that a data subject can mandate a properly qualified not-for-profit body to seek compensation on his/her behalf.

DRI **recommends** that the Heads of Bill be amended to provide that a properly qualified not-for-profit body shall have the right to lodge a complaint or seek an injunction against a controller/processor if it considers that the rights of a data subject have been infringed.

---

[9] [2010] IEHC 221.

Joint Committee on Justice and Equality
Opening Statement
Dr. Geoffrey Shannon, Special Rapporteur on Child Protection

I would like to take this opportunity to thank the Committee for the invitation to address it on the General Scheme of the Data Protection Bill 2017.

Introduction

The General Scheme of the Data Protection Bill 2017 is a crucial step in Ireland's preparation for the implementation of new EU data protection obligations and it provides a much-needed update of existing data protection legislation in this jurisdiction, namely the Data Protection Acts 1988 and 2003.

The two key pieces of European legislation reflected in the General Scheme are the EU General Data Protection Regulation (EU) 2016/679 and Directive (EU) 2016/680 on the use of personal data by criminal enforcement authorities. The General Data Protection Regulation (GDPR) was agreed in 2016 and mandates higher data protection standards for data subjects, imposing increased obligations on data controllers and processors. It focuses on reinforcing individual's rights; ensuring stronger enforcement of data protection rules; and streamlining international transfers of personal data.[1]

As a Regulation, the GDPR will take effect in this jurisdiction automatically from 25 May 2018 and does not require transposition. Nevertheless the 2017 Bill significantly gives effect to its provisions and provides for derogations where permitted.

Developments in the 2017 Bill as they relate to Children's Rights

From a children's rights perspective, certain aspects of the 2017 General Scheme and its interaction with the EU GDPR require particular consideration – namely:

- the age of digital consent - which I believe should be set at 13;
- the need for a definition of "preventative and counselling services" - so that blanket blocking of sites does not prevent access to much needed, and increasingly online services for young people;
- the right to be forgotten – which is as much a child's right as an adults, and arguably has greater impact;
- the link between data protection rights and digital safety – particularly in the context of cyber-bullying and adult data literacy; and
- the processing of sensitive personal data.

In addition, it would be interesting to know whether children have been canvassed in respect of this Bill, and how they perceive its current form.

It must be remembered that children, like adults, have data protection rights under both EU laws and under the existing Irish data protection regime. Children may not, however, depending on their age and their level of maturity and understanding, be in a position

[1] European Commission, 'Fact Sheet Questions and Answers Data protection reform' <http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm> accessed 14 November 2016.

independently to exercise these rights. In this vein, and throughout the discussion herein, it is necessary to bear in mind Recital 38 of the GDPR. It provides as follows:

> Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

It goes on to state that that such specific protection should particularly apply to the use of children's personal data for the purposes of marketing or creating personality or user profiles and the collection of such personal data of children when using services offered directly to a child. Recital 38 also states that the consent of the holder of parental responsibility for the child should not be necessary in the context of "preventative or counselling services offered directly to a child". This Recital explicitly recognises children as a separate and particularly vulnerable group in society with regard to data protection issues, and I believe that it must inform the approach taken in the 2017 Bill in relation to the protection of the personal data of children.

The Digital Age of Consent

Part 3 of the General Scheme of the Data Protection Bill 2017 sets out the Heads required to give further effect to the GDPR. Head 16 is particularly relevant from a child protection perspective. It concerns "child's consent in relation to information society services" and relates to Article 8 of the GDPR which sets the age under which children require parental consent to sign up to digital services – known as "the digital age of consent". Pursuant to Article 8, where a child is below the age of 16 years, data processing shall only be lawful to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member states, however, have discretion to provide by law for a lower age, once that lower age is not below 13 years. When the age of consent is set, the data controller is obligated to make reasonable efforts to verify in respect of children below the age of consent that such consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

The requirement for a digital age of consent acknowledges that children are often unaware of the risks associated with internet use, as well as the consequences of the processing of their personal data. As their competencies grow, however, this situation changes.

Article 5 of the UN Convention on the Rights of the Child (UNCRC) explicitly recognises that children have evolving capacities and that as they get older they have a greater ability to take responsibility for decisions affecting their lives.[2] The aim of the GDPR in setting a digital age of consent is to protect young people from commercial online marketing providers, for instance social media and gaming platforms. The current situation whereby the same data practices are being used to target teenagers as those used to target adults is unacceptable.[3]

---

[2] Gerison Lansdown, 'The evolving capacities of the child' (UNICEF Innocent Insight, 2005) <https://www.unicef-irc.org/publications/pdf/evolving-eng.pdf> accessed 15 November 2016, ix.

[3] Sonia Livingstone, 'Sonia Livingstone on the GDPR, No more social networking for teens?' (Better Internet for Kids, 31 March 2016). <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=687352> accessed 15

In Head 16 of the General Scheme of the 2017 Bill, in its current form, the Irish digital age of consent has not yet been set out. It is silent in this regard. In the explanatory notes to the Head, a consultation process on the appropriate age threshold is described as having been completed and it was indicated that the results of same will be submitted to the government for a decision in due course.

It appears, therefore, that no determination on this issue has been made by the legislature at this point in time. In this regard, I believe that Ireland should take the opportunity now to designate the lowest permissible age – namely 13 – as the age of digital consent for our jurisdiction. This lower digital age of consent has also been recommended by children's organisations such as the Children's Rights Alliance. Indeed, there are a variety of competing children's rights and practical realities that support the argument that the appropriate age, having regard to the permissible age range delineated by the GDPR, should be the lowest possible. A discussion of the relevant rights is set out below.

Right to participate

The right of the child to participate and be heard in proceedings concerning him or her is a fundamental principle of international children's rights law and is enshrined by Article 12 of the UNCRC. It states as follows:

> State Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.[4]

The right of participation is similarly reflected in the EU Fundamental Rights Charter, applicable when Member States apply EU Regulations directly. Article 24 thereof provides as follows:

> Children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity.[5]

The importance of the voice of the child and the child's right to participate has been promoted recently in this jurisdiction through the Children's Amendment in Article 42A of the Irish Constitution and throughout the provisions of the Children and Family Relationships Act 2015. The focus, however, has primarily been on these rights in the context of legal proceedings concerning the child, such as guardianship, access and custody proceedings.[6] These rights should also be considered and respected in the creation of legislation which will affect children – such as the drafting of the Data Protection Bill 2017.

November 2016. She refers to practices such as cross platform, mobile location tracking and productive analytics as examples.

[4] Article 12, UNCRC.

[5] Article 21(1), EU Fundamental Rights Charter.

[6] Section 31(2) of the Guardianship of Infants Act 1964, as inserted by s.63 of the Children and Family Relationships Act 2015 provides that in determining what is in the best interests of the child, the court is

In line with the National Policy Framework, a strategy was developed concerning the participation of young persons - *The National Strategy on Children and Young People's Participation in Decision-Making 2015-2020.* Its goal is to ensure that children and young people have a voice in their individual and collective everyday lives and it explicitly acknowledges their voice in decision-making requires a cross-Government response, with initiatives and actions from all key departments and agencies.

With the National Strategy and the recommendation of the UN Committee in mind, it is unclear whether or not children have been consulted on the issue of Ireland's proposed digital age of consent. While the explanatory note to Head 16 describes a "consultation process on the appropriate age threshold" which it declares as having already been completed, there is no comment in the explanatory note on *what* this consultation process entailed and in particular, *who* it involved. In light of the child's right of participation, I believe that the views of at the very least a focus group of Irish children must first be garnered before any final decision is made on this question. Given the integral role that information services technology and digital media plays in the lives of our young people, as exhibited in the statistics in the attached submission, it is critical that they be given an opportunity to voice their view on the matter. I therefore recommend that a consultation process take place to ascertain the views of a variety of age groups of Irish children on the issue of digital consent.

Freedom of expression

The right to freedom of expression is a human right that is not confined in its remit to adults. The UN Convention on the Rights of the Child guarantees a child's enjoyment to freedom of expression in Article 13 as follows:

> The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.[7]

Further related rights under the UNCRC include the right to access appropriate information, provided in Article 17, and the freedom to assemble peacefully. Such assembly may take place in the context of an online environment. These rights, therefore, are often exercised by children through their use of information and communications technology.

In a number of my previous rapporteur reports, I have highlighted the importance of the internet for children's freedom of information. Whilst there is a genuine need, and indeed obligation, to protect children from the dangers of the internet, the Irish State must ensure that it does not unreasonably restrict children's civil and political rights such as the right to freedom of information and expression. The Children's Rights International Network (CRIN) identifies instances whereby internet service providers are pressured by State authorities to institute blanket filters to block websites containing material which is argued to be unsuitable for under-18s. Yet some of the sites contain material which could be important

---

mandated to have regard to the views of the child that are ascertainable, whether in accordance with s.32 or otherwise.

[7] Article 13(1), UNCRC.

for the well-being of many under-18s such as material on sex education, politics and support groups for alcohol dependency and suicide. These blanket filters are arguably contrary to CRC Article 5, which requires that children are facilitated to exercise their rights in line with their evolving capacities.

Restricting internet usage for children, for instance by setting the digital age of consent at 16, should therefore be approached with caution and the varying rights at play must be borne in mind. The overarching consideration must be whether any such restriction is in the best interests of the child. This is mandated in Article 24 of the EU Charter of Fundamental Rights which provides that in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration. I believe that to prevent any infringement of the child's right to freely express him or herself and to ensure children's access to online information, Ireland should avoid setting the digital age of consent at 16. Classifying the age of consent at 13 would be preferable to prevent a dramatic reduction in the participation of young people in online services. Given that Head 16 of the General Scheme requires the data controller to make "reasonable efforts" to verify that the consent of those under the designated age threshold is given or authorised by the holder of parental responsibility over the child, it can be anticipated that controllers will try to relieve themselves of any burden to seek parental consent. They may, for instance, simply change their age limits to the relevant age of digital consent across the board and in this way, place a blanket ban on those under that age accessing their online service. Furthermore, it is unclear how "reasonable efforts" will be interpreted and this is an issue that requires further consideration. The inclusion of the phrase "taking into consideration available technology" may give businesses that are in control of that technology an opt-out option.

Given the significant percentage of children who are active online, setting a high digital age of consent at 16 could prevent all those younger than this age from accessing material online. While the number of children using information and services technology is still high in the 9 to 12 age range, designating the age of digital consent at 13, the lowest permissible level by the GDPR, would have a lesser overall impact on the exercise by children of their right of freedom of expression.

Practical considerations concerning the digital age of consent

Definition of preventative and counselling services

The rights of the child discussed above, namely to participate in matters concerning them, to be heard, to express themselves freely and to access information, need to be exercised effectively by children. On a practical level, therefore, certain realities must be considered to ensure that children are capable of exercising these rights in the context of their online activity and use of digital services. A difficulty may arise in circumstances where the view of the child is not aligned to the view of his or her parents or guardians. Children for instance may wish to access online services in relation to sexual education or health, to explore LGBT issues or to seek support if they are being bullied. Certain service providers in these areas regularly require and retain personal data from the young persons who access their service in order to improve and fine tune the operation and content of same – thus children's personal data may be processed and retained.

These types of issues may be ones which the children involved, for a variety of reasons, may not be comfortable discussing with their parents or guardians. Children and young people often contact organisations/services in confidence and arguably should be allowed to continue to do so without having to obtain consent from their parent. If the digital age of consent was to be set at 16, this would in all likelihood operate to prevent children from accessing these services – something which cannot be said to be in their best interests. Even with the age of consent being set at 13, there is still a possibility that those children under the age of 13 will be unable to access the online service they wish to view or use due to an inability to request consent from their parent/guardian because of the nature of the website to which access is sought.

While Recital 38 of the GDPR specifically provides that the special rules relating to the processing of children's personal data – namely the requirement for parental consent – should not apply in the context of preventative or counselling services offered directly to a child, whether the variety of service providers envisaged above will come within the definition of "preventative or counselling services" remains to be seen.

In this vein, therefore, it is recommended that consideration be given to defining "preventative or counselling services" for the purpose of the 2017 Bill. A broad definition should be applied to this phrase to ensure that the types of websites envisaged above fall within this exception to the general specialised protection envisaged for children by the GDPR.

It will be also necessary to provide clarification on whether organisations that provide online support services to children will have to verify the consent of the child's holder of parental responsibility before processing a child's data for not-for-profit use.

Holder of parental responsibility – a wider definition required

It should be noted that Head 16 of the General Scheme of the 2017 Bill does not contain any definition of the phrase "the holder of parental responsibility over the child". This term is taken directly from the GDPR and has no clear meaning under Ireland's existing statutes concerning children. Clarification is thus required so that those persons who fall within this term are clearly identified.

It is submitted therefore, that the "holder of parental responsibility" should include any parent and any guardian of the child, whether automatic or court appointed pursuant to the provisions of the Guardianship of Infants Act 1964, as amended by the Children and Family Relationships Act 2015. This would include temporary guardians, testamentary guardians and those appointed under s.6C of the 1964 Act. Applying a wide definition to this phrase is preferable to allow a broader category of persons who may be responsible for a child to be able to give the requisite consent for the child in question. It may ensure that children under 13 have a greater pool of persons from whom consent to sign up to digital services can be authorised.

A further concern with regard to the involvement of the "holder of parental responsibility" is that many parents or guardians of children have lower digital literacy skills compared with their child. Despite this, the GDPR places the responsibility to manage children's data

protection on their parents and guardians where the child is under the digital age of consent. It is recommended that awareness needs to be raised in relation to the proposed digital age of consent, the meaning of data protection and processing, and the consequences of same.

In the Department of Justice and Equality's Consultation Paper on *Data protection safeguards for children ("digital age of consent"),* published in November 2016, it noted that the GDPR requires that activities addressed to children must in future be given specific attention. It stated that this necessitates the development of appropriate child-friendly materials by the Data Protection Commission which "convey an understanding not only of the risks that may arise when personal information is supplied online but also the remedies that are available under data protection law."[8]

Right to be forgotten

In my ninth rapporteur report, I discussed the right to be forgotten and its importance from the perspective of a child.[9] The right to be forgotten was held to exist in the seminal case of *Google v Spain*.[10] In that decision, the European Court of Justice held that an EU citizen has the right to request that commercial search firms, such as Google, remove links to their personal information when requested, provided that the information is no longer relevant – emphasising an individual's right to privacy which overrides the public interest in access to information in certain circumstances. Article 17 of the GDPR concerns the "right to erasure", known as the right to be forgotten. There is no specific Head in the General Scheme that gives particular effect to Article 17 of the GDPR.

The right to be forgotten is not just an important right which may be exercised by adults. It is even more relevant for children. This is particularly so as children are less likely than adults to be aware that information they post online may be available long-term and they may not consider the consequences of posting something online which may last long beyond their childhood. While not stated in Article 17 of the GDPR, it is suggested that Ireland should take the opportunity to include specific provisions on this issue in the 2017 Data Protection Bill. The relevance for children of the "right to be forgotten" should be acknowledged, children should be educated about the matter, and it should be understood that the age at which an individual posts information online should be considered a very important factor in decisions about whether to remove an individual's personal information from sites.

Cyber-harassment and misuse of personal data

The GDPR and the General Scheme of the 2017 Bill cannot be considered in a vacuum. There are risks associated with young people maintaining an online presence which cannot be ignored. In this vein, the introduction of the Criminal Law (Sexual Offences) Act 2017 is

[8] Department of Justice and Equality, Data protection safeguards for children ('digital age of consent') Consultation Paper http://www.justice.ie/en/JELR/Consultation_paper_Digital_Age_of_Consent.pdf/Files/Consultation_paper_Digital_Age_of_Consent.pdf, at para 7.

[9] Geoffrey Shannon, *Ninth Report of the Special Rapporteur on Child Protection* (2016).

[10] *Google Spain, S.L., Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* ECLI:EU:C:2014:317.

to be welcomed and applauded. This Act demonstrates Ireland's commitment to better protecting its children from online predators and it specifically recognises the dangers that come with technological advances by creating a wide range of new criminal offences dealing with child pornography and grooming, with a particular emphasis on the use of information and communication technology in such offences. A further concern associated with children's internet usage is the prevalence of cyber-bullying or harassment. The prevalence of cyber-harassment is something which I considered in detail in my sixth rapporteur report.[11] The problem is widespread – one EU study indicated that 21% of children have been exposed to potentially harmful user-generated content such as hate, pro-anorexia and self-harm.[12]

In order to ensure that children are protected from cyber-bullying in their online activities and to ensure that their personal data is not exploited, regard should be had to the recommendation of the UN Committee on the Rights of the Child that States should "develop effective safeguards for children against abuse without unduly restricting the full enjoyment of their rights". It is notable that Article 6(2) of the GDPR enables Member States to "maintain or introduce more specific provisions to adapt the application of the rules…to ensure lawful and fair processing." This relates to data processing that is necessary for compliance with a legal obligation to which the data controller is subject or to processing that is necessary for the performance of a task carried out in the public interest. Having regard to Article 6(2) and the concerns raised above, I believe that further exploration is merited to ascertain whether these rules, or other mechanisms, could be used to enable the State to put specific legislative protection or exceptions in place to protect the right of children to participate online without having their data used for commercial gain.

To further address the issues raised above concerning cyber-harassment and bullying, I believe that regard should be had to the recommendations I have recently made in my tenth rapporteur report.[13]

I also endorse the recommendations of the Law Reform Commission in its 2016 Report on Harmful Communications and Digital Safety concerning "take down procedures" – a mechanism to ensure the efficient removal of harmful digital communications online.[14] The proposed Office of the Digital Safety Commissioner of Ireland would therefore oversee an "effective and efficient" take down procedure in a timely manner, regulating for a system of take down orders in respect of harmful cyber communications made in respect of both adults and children. Its regulatory role would apply to a wide range of digital or online service providers, including any undertaking that provides a digital or online service, whether by the internet, a telecommunications system, the world wide web or otherwise.

Included in the role of the Digital Safety Commissioner would be to publish a Code of Practice on Take Down Procedures for Harmful Communications.

[11] Geoffrey Shannon, *Sixth Report of the Special Rapporteur on Child Protection* (2013), at section 2.2.
[12] EU Kids Online network, available at: www.eukidsonline.net (last accessed 1 December 2015). Funded by the European Commission Safer Internet Programme (2009-11).
[13] Geoffrey Shannon, *Tenth Report of the Special Rapporteur on Child Protection* (2017), at section 2.2.
[14] LRC 116-2016 Report on Harmful Communications and Digital Safety.

The proposal made by the Law Reform Commission regarding the establishment of a new statutory oversight system as detailed above appears to be a practical and viable solution to the current lacuna in the law. It is recommended therefore that consideration be given by the government to Chapter 3 of the Commission's Report forthwith, to enable progress to be made in this regard and to ensure that steps are taken to establish an Office of the Digital Safety Commissioner.

It is further recommended, in light of the publication of the General Scheme of the 2017 Data Protection Bill that the Digital Safety Commissioner, if established, should be required to liaise with the Data Protection Commission operating pursuant to the 2017 Data Protection Bill. Cooperation between the two bodies would be essential to ensure that harmful communications are removed and potential breaches of data protection legislation investigated.

Processing of special categories of data

Article 9 of the GDPR concerns the processing of "special categories of personal data". It provides as follows:

> Processing of 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 shall be prohibited.[15]

Such processing, however, is permitted in a number of specified circumstances as set out in Article 9.2, including where the processing of such personal data is necessary for the provision of health or social care or treatment or the management of health or social care systems and services,[16] subject to suitable and specific measures being implemented to safeguard the fundamental rights and freedoms of data subjects. In the General Scheme of the 2017 Bill, Heads 17 and 18 concern the processing of these special categories of data. Head 17 permits the making of regulations concerning the processing of sensitive data where "necessary for reasons of substantial interest", and Head 18, Sub-head 1 particularly provides that these categories of sensitive data may be processed where necessary for, inter alia, "the management of health and social care systems and services and for public interest reasons in the area of public health."

It can be imagined that the abovementioned exceptions to the prohibition of the processing of sensitive personal data will enable the Child and Family Agency (CFA) to process such data in the carrying out of its statutory role. This will inevitably include special sensitive data relating to children and young persons. The 2017 Bill only allows this processing to take place on the condition that suitable and specific measures are adhered to in order to safeguard the fundamental rights and interests of the data subject. As identified in the explanatory notes to Head 18, it is as of yet unclear as to the extent to which the "suitable and specific safeguards" referred to in Article 9 and included in the Bill are intended to be additional or complementary safeguards to those already placed upon data controllers

[15] Article 9.1 GDPR.
[16] Article 9.2(h).

elsewhere in the GDPR or whether additional safeguards will be required. Given the nature of the data involved, it is recommended that consideration be given to the inclusion of additional safeguards, particularly where a child's sensitive personal data is engaged and is to be processed by the CFA. This should be explored having regard to Recital 38 of the GDPR and the special protection required therein for the personal data of children.

I would like to thank you very much for taking time to listen to me and I would be happy to answer any questions you might have.

Dr. Geoffrey Shannon
28 June 2017

Joint Committee on Justice and Equality
Submission
Dr. Geoffrey Shannon, Special Rapporteur on Child Protection

Introduction

The General Scheme of the Data Protection Bill 2017 was published by the former Minister for Justice and Equality, Frances Fitzgerald T.D., and the former Minister of State for Data Protection, Dara Murphy T.D., on the 12th of May 2017. It is a crucial step in Ireland's preparation for the implementation of new EU data protection obligations and it provides a much-needed update of existing data protection legislation in this jurisdiction, namely the Data Protection Acts 1988 and 2003. Upon its publication, Dara Murphy T.D. stated the following:

> Data protection concerns the right that we all have to the safeguarding of our personal information and its use, for the protection of our personal privacy… Government approval for the drafting of the Data Protection Bill 2017 is an important step in Ireland's ongoing preparations to implement new EU data protection rules agreed last year.

The two key pieces of European legislation reflected in the General Scheme are the EU General Data Protection Regulation (EU) 2016/679 and Directive (EU) 2016/680 on the use of personal data by criminal enforcement authorities. The General Data Protection Regulation (GDPR) was agreed in 2016 and mandates higher data protection standards for data subjects, imposing increased obligations on data controllers and processors. It focuses on reinforcing individual's rights; ensuring stronger enforcement of data protection rules; and streamlining international transfers of personal data.[17] As a Regulation, the GDPR will take effect in this jurisdiction automatically from 25 May 2018 and does not require transposition. Nevertheless the 2017 Bill significantly gives effect to its provisions and provides for derogations where permitted. The General Scheme also transposes the content of the law enforcement Directive which concerns the processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences, and the free flow of such data. While the general concepts contained in the Regulation and Directive are broadly similar to those set out in Ireland's existing data protection legislation, the new EU measures mandate improvements to our data protection regime. The 1988 and 2003 Acts, therefore, will be largely superseded by the GDPR and Part 4 of the 2017 Bill.[18]

Developments in the 2017 Bill

There are a number of key developments proposed in the General Scheme of the Data Protection Bill 2017, which gives an outline of the legislation that we can expect to be introduced on certain aspects of the GDPR. These include the establishment of a Data Protection Commission (DPC) which may have up to three Commissioners; the expansion of the powers of the DPC to supervise and enforce the new enhanced EU standards; and the obligation on individual data controllers and processors to put appropriate technical and

[17] European Commission, 'Fact Sheet Questions and Answers Data protection reform' <http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm> accessed 14 November 2016.
[18] See Head 5, General Scheme of the Data Protection Bill 2017.

organisational measures in place in order to ensure that their processing of personal data complies with the GDPR. It also contains provisions relating to the processing of historic and scientific data and data relating to criminal convictions. From a children's rights perspective, however, certain aspects of the 2017 General Scheme and its interaction with the GDPR require particular consideration – namely, the age of digital consent, the right to be forgotten, the link between data protection rights and digital safety, and the processing of sensitive personal data. It is important to note that the GDPR is the overarching piece of legislation for the purposes of this consideration in that the 2017 Bill simply deals with aspects of its implementation and derogation.

It must be remembered that children, like adults, have data protection rights under both EU laws and under the existing Irish data protection regime. Children may not, however, depending on their age and their level of maturity and understanding, be in a position independently to exercise these rights. In this vein, and throughout the discussion herein, it is necessary to bear in mind Recital 38 of the GDPR. It provides as follows:

> Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

It goes on to state that that such specific protection should particularly apply to the use of children's personal data for the purposes of marketing or creating personality or user profiles and the collection of such personal data of children when using services offered directly to a child. Recital 38 also states that the consent of the holder of parental responsibility for the child should not be necessary in the context of "preventative or counselling services offered directly to a child". This Recital explicitly recognises children as a separate and particularly vulnerable group in society with regard to data protection issues, and I believe that it must inform the approach taken in the 2017 Bill in relation to the protection of the personal data of children.

Children and digital rights

In 2015, the Human Rights Council discussed freedom of opinion and expression and freedoms of peaceful assembly and of association, including the right to seek, receive, and impart information online[19] - an emerging human rights issue which is as yet little understood. It is particularly under-explored in the context of children's rights.

The human rights consequences for matters such as online surveillance by governments can be grave for ordinary citizens, including children. The right to privacy, the right to freedom of expression as well as the right to life can be at issue in States in which political dissent is forbidden by governments.[20] The human rights debates around such matters often fail to consider threats specific to children, such as online abuse. Nevertheless, child protection

[19] See http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16095&LangID=E.

[20] See Children's Rights International Network, https://www.crin.org/en/home/what-we-do/crinmail/childrens-rights-united-nations-142#digital_rights and A. Daly, *A Commentary on the United Nations Convention on the Rights of the Child, Article 15: The Right to Freedom of Association and Peaceful Assembly* (Monograph–Martinus Nijhoff Publishers, 2016).

arguments are often used to justify censorship. These challenging issues must be considered in a children's rights context.

All citizens, including children, must have free and equal access to the Internet. This concerns physical and economic barriers, but also the question of who controls access to the Internet, as often private companies attempt to restrict free and equal access by trying to decrease "net neutrality" – the principle that all data should be treated equally whether it derives from a large company or a small NGO. Without net neutrality, "fast lanes" could be created by Internet service providers, facilitating fee-paying websites to offer a faster connection to users. Websites of organisations which cannot afford to pay for such a service would load so slowly as to be unusable. This would also affect internet users' access to all websites, including those of small NGOs which are crucial for facilitating children's rights. The European Parliament voted in 2015 against rules intended to safeguard net neutrality in the EU.[21] It is positive, however, that Irish authorities have indicated unwillingness to retreat from net neutrality[22] and they should continue to do so to the extent possible, not least to uphold the ability of small groups and organisations to facilitate the progression of children's rights.

Having regard to statistics in respect of internet usage, it is unsurprising that children are a very active group online. Globally, children represent almost a third of internet users and internet usage amongst children in Ireland exceeds the European average.[23] There is no doubt that children are highly engaged with digital media and technology, as demonstrated in a recent study compiled by O'Neill and Dinh.[24] Their research exhibits that three in five children have a social networking profile; 86% of 9-year-olds having a computer in their home; and one third of 9 to 10-year-olds go online daily. For 15 to 16-year-olds, three quarters of them use the internet every day. Children therefore undeniably represent a significant online presence.

The Digital Age of Consent

Part 3 of the General Scheme of the Data Protection Bill 2017 sets out the Heads required to give further effect to the GDPR. Head 16 is particularly relevant from a child protection perspective. It concerns "child's consent in relation to information society services" and relates to Article 8 of the GDPR which sets the age under which children require parental consent to sign up to digital services – known as "the digital age of consent". Pursuant to Article 8, where a child is below the age of 16 years, data processing shall only be lawful to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member states, however, have discretion to provide by law for a lower age, once that lower age is not below 13 years. When the age of consent is set, the data controller is obligated to make reasonable efforts to verify in respect of children below the age of consent that such consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. Thus, under the GDPR, the

[21] http://www.bbc.com/news/technology-34649067.

[22] http://www.independent.ie/business/technology/government-set-to-oppose-any-moves-to-water-down-net-neutrality-30771031.html.

[23] Sonia Livingstone, John Carr and Jasmina Byrne, 'One in Three: Internet Governance and Children's Rights' Innocenti Discussion Paper No.2016-01, UNICEF Office of Research, Florence, 2016.

[24] Brian O'Neill and Thuy Dinh, 'Social Networking Among Irish 9-16 Year Olds' (Arrow@DIT, 28 June 2012) <http://arrow.dit.ie/cgi/viewcontent.cgi?article=1028&context=cserrep> accessed 3 November 2016, 1.

digital age of consent to the collection and processing of personal data is 16, but Member States have discretion to set their own national limit at any age between 13 and 16.

The requirement for a digital age of consent acknowledges that children are often unaware of the risks associated with internet use, as well as the consequences of the processing of their personal data. As their competencies grow, however, this situation changes. Article 5 of the UN Convention on the Rights of the Child explicitly recognises that children have evolving capacities and that as they get older they have a greater ability to take responsibility for decisions affecting their lives.[25] The aim of the GDPR in setting a digital age of consent is to protect young people from commercial online marketing providers, for instance social media and gaming platforms. The current situation whereby the same data practices are being used to target teenagers as those used to target adults is unacceptable.[26]

At present, the existing Data Protection Acts of 1988 and 2003 do not set a minimum age at which a person can give his or her consent to the processing of his or her data in this jurisdiction. Section 2A(1) of the 1988 Act, as amended, provides that where a person "by reason of his or her physical or mental incapacity or age" is or is likely to be unable to appreciate the nature and effect of giving consent, such consent may be given by a parent or guardian or a grandparent, uncle, aunt, brother or sister of the person provided that the giving of such consent is not prohibited by law. This is a broad approach which avoids establishing any minimum age of digital consent. In the 2017 Bill, however, such an age must be designated in line with the GDPR. At this stage, it is not a question of whether the setting of a digital age of consent is the best course of action to take in respect of the processing of children's personal data – this has been mandated by the GDPR and from May 2018, the age of digital consent will be 16 unless Ireland choses to derogate and select a lower age. In Head 16 of the General Scheme of the 2017 Bill, in its current form, the Irish digital age of consent has not yet been set out. It is silent in this regard. In the explanatory notes to the Head, a consultation process on the appropriate age threshold is described as having been completed and it was indicated that the results of same will be submitted to the government for a decision in due course.

It appears, therefore, that no determination on this issue has been made by the legislature at this point in time. In this regard, I believe that Ireland should take the opportunity now to designate the lowest permissible age – namely 13 – as the age of digital consent for our jurisdiction. This lower digital age of consent has also been recommended by children's organisations such as the Children's Rights Alliance. Indeed, there are a variety of competing children's rights and practical realities that support the argument that the appropriate age, having regard to the permissible age range delineated by the GDPR, should be the lowest possible. A discussion of the relevant rights is set out below.

---

[25] Gerison Lansdown, 'The evolving capacities of the child' (UNICEF Innocent Insight, 2005) <https://www.unicef-irc.org/publications/pdf/evolving-eng.pdf> accessed 15 November 2016, ix.

[26] Sonia Livingstone, 'Sonia Livingstone on the GDPR, No more social networking for teens?' (Better Internet for Kids, 31 March 2016). <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=687352> accessed 15 November 2016. She refers to practices such as cross platform, mobile location tracking and productive analytics as examples.

Right to participate

The right of the child to participate and be heard in proceedings concerning him or her is a fundamental principle of international children's rights law and is enshrined by Article 12 of the UNCRC. It states as follows:

> State Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.[27]

The right of participation is similarly reflected in the EU Fundamental Rights Charter, applicable when Member States apply EU Regulations directly. Article 24 thereof provides as follows:

> Children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity.[28]

The Children's Rights International Network (CRIN) considered the participation of European children in matters affecting them in its report. Children strongly believe that they should have a say in the important decisions affecting them, but they face many obstacles, including adult indifference and the lack of knowledge about participation rights amongst both adults and children. Formal structures established for children's participation must function well and avoid tokenism. Otherwise they "create a feeling of frustration."[29] Children report feeling most heard in their families, but they often report feeling least heard by politicians.[30] Many wish to have greater opportunities to better participate in their local community and relevant services such as health care provision, yet they report that they "are often not aware of what support and activities are on offer or how to access them, let alone how to have a say in what services should be provided or how."

The importance of the voice of the child and the child's right to participate has been promoted recently in this jurisdiction through the Children's Amendment in Article 42A of the Irish Constitution and throughout the provisions of the Children and Family Relationships Act 2015. The focus, however, has primarily been on these rights in the context of legal proceedings concerning the child, such as guardianship, access and custody proceedings.[31] These rights should also be considered and respected in the creation of legislation which will affect children – such as the drafting of the Data Protection Bill 2017. In April 2014, the Government made commitments in the area of child participation as the

[27] Article 12, UNCRC.
[28] Article 21(1), EU Fundamental Rights Charter.
[29] Report cited in Ecorys/University of West of England/Child-to-Child, *Evaluation of Legislation, Policy and Practice on Child Participation in the EU* (European Commission, 2015).
[30] YouthLink Scotland, *Being Young in Scotland* (YouthLink Scotland, 2009).
[31] Section 31(2) of the Guardianship of Infants Act 1964, as inserted by s.63 of the Children and Family Relationships Act 2015 provides that in determining what is in the best interests of the child, the court is mandated to have regard to the views of the child that are ascertainable, whether in accordance with s.32 or otherwise.

Department of Children and Youth Affairs launched '*Better Outcomes Brighter Future: Report of the National Policy Framework for Children and Young People 2014-2020'.* The Framework has as its objective the setting out of "transformation goals and outcomes for children and young people and new structures reporting to the Cabinet Committee on Social Policy." The Minister for Children and Youth Affairs stated that the Framework is about "moving on from addressing the legacy of failings to promoting a new culture and cross-government approach to improving outcomes for all children."[32]

In line with the National Policy Framework, a strategy was developed concerning the participation of young persons - *The National Strategy on Children and Young People's Participation in Decision-Making 2015-2020.* Its goal is to ensure that children and young people have a voice in their individual and collective everyday lives across the five national outcome areas and it explicitly acknowledges that giving children and young people a voice in decision-making requires a cross-Government response, with initiatives and actions from all key departments and agencies. This Strategy reflects the UN Committee on the Rights of the Child's recommendation that all States ensure that children are consulted so that their views and experiences can be taken into account in "developing laws, policies, programmes, and in the setting up of services, and other measures relating to digital media and informational technology".[33]

With the National Strategy and the recommendation of the UN Committee in mind, it is unclear whether or not children have been consulted on the issue of Ireland's proposed digital age of consent. While the explanatory note to Head 16 describes a "consultation process on the appropriate age threshold" which it declares as having already been completed, there is no comment in the explanatory note on *what* this consultation process entailed and in particular, *who* it involved. In light of the child's right of participation, I believe that the views of at the very least a focus group of Irish children must first be garnered before any final decision is made on this question. Given the integral role that information services technology and digital media plays in the lives of our young people, as exhibited in the abovementioned statistics, it is critical that they be given an opportunity to voice their view on the matter. I therefore recommend that a consultation process take place to ascertain the views of a variety of age groups of Irish children on the issue of digital consent.

Freedom of expression

The right to freedom of expression is a human right that is not confined in its remit to adults. The UN Convention on the Rights of the Child guarantees a child's enjoyment to freedom of expression in Article 13 as follows:

> The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of

[32] http://www.dcya.gov.ie/viewdoc.asp?DocID=3151.

[33] Committee on the Rights of the Child, 'Report of the 2014 Day of General Discussion "Digital media and children's rights"' (UNCRC, 2014) <http://www.ohchr.org/EN/HRBodies/CRC/Pages/Discussion2014.aspx> accessed 14 November 2016, 21.

> frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.[34]

Further related rights under the UNCRC include the right to access appropriate information, provided in Article 17, and the freedom to assemble peacefully. Such assembly may take place in the context of an online environment. These rights, therefore, are often exercised by children through their use of information and communications technology.

In a number of my previous rapporteur reports, I have highlighted the importance of the internet for children's freedom of information. Whilst there is a genuine need, and indeed obligation, to protect children from the dangers of the internet, the Irish State must ensure that it does not unreasonably restrict children's civil and political rights such as the right to freedom of information and expression. CRIN identifies instances whereby internet service providers are pressured by State authorities to institute blanket filters to block websites containing material which is argued to be unsuitable for under-18s. Yet some of the sites contain material which could be important for the well-being of many under-18s such as material on sex education, politics and support groups for alcohol dependency and suicide. These blanket filters are arguably contrary to CRC Article 5, which requires that children are facilitated to exercise their rights in line with their evolving capacities. For some under-18s, access to such sites will provide them with crucial help and support. Indeed, it is important to acknowledge and highlight the benefits of digital activity for young persons. In a recent report by OFCOM, the UK Communications Regulator, a number of advantages of internet usage amongst children were identified – it can encourage peer-to-peer sharing; promote involvement in civic activities; and support different forms of offline learning and creativity, such as learning a musical instrument.

Restricting internet usage for children, for instance by setting the digital age of consent at 16, should therefore be approached with caution and the varying rights at play must be borne in mind. The overarching consideration must be whether any such restriction is in the best interests of the child. This is mandated in Article 24 of the EU Charter of Fundamental Rights which provides that in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration. I believe that to prevent any infringement of the child's right to freely express him or herself and to ensure children's access to online information, Ireland should avoid setting the digital age of consent at 16. Classifying the age of consent at 13 would be preferable to prevent a dramatic reduction in the participation of young people in online services. Given that Head 16 of the General Scheme requires the data controller to make "reasonable efforts" to verify that the consent of those under the designated age threshold is given or authorised by the holder of parental responsibility over the child, it can be anticipated that controllers will try to relieve themselves of any burden to seek parental consent. They may, for instance, simply change their age limits to the relevant age of digital consent across the board and in this way, place a blanket ban on those under that age accessing their online service. Furthermore, it is unclear how "reasonable efforts" will be interpreted and this is an issue that requires further consideration. The inclusion of the

[34] Article 13(1), UNCRC.

phrase “taking into consideration available technology” may give businesses that are in control of that technology an opt-out option.

Given the significant percentage of children who are active online, setting a high digital age of consent at 16 could prevent all those younger than this age from accessing material online. While the number of children using information and services technology is still high in the 9 to 12 age range, designating the age of digital consent at 13, the lowest permissible level by the GDPR, would have a lesser overall impact on the exercise by children of their right of freedom of expression.

Practical considerations concerning the digital age of consent

The rights of the child discussed above, namely to participate in matters concerning them, to be heard, to express themselves freely and to access information, need to be exercised effectively by children. On a practical level, therefore, certain realities must be considered to ensure that children are capable of exercising these rights in the context of their online activity and use of digital services. A difficulty may arise in circumstances where the view of the child is not aligned to the view of his or her parents or guardians. Children for instance may wish to access online services in relation to sexual education or health, to explore LGBT issues or to seek support if they are being bullied. Certain service providers in these areas regularly require and retain personal data from the young persons who access their service in order to improve and fine tune the operation and content of same – thus children’s personal data may be processed and retained.

These types of issues may be ones which the children involved, for a variety of reasons, may not be comfortable discussing with their parents or guardians. Children and young people often contact organisations/services in confidence and arguably should be allowed to continue to do so without having to obtain consent from their parent. If the digital age of consent was to be set at 16, this would in all likelihood operate to prevent children from accessing these services – something which cannot be said to be in their best interests. Even with the age of consent being set at 13, there is still a possibility that those children under the age of 13 will be unable to access the online service they wish to view or use due to an inability to request consent from their parent/guardian because of the nature of the website to which access is sought. While Recital 38 of the GDPR specifically provides that the special rules relating to the processing of children’s personal data – namely the requirement for parental consent – should not apply in the context of preventative or counselling services offered directly to a child, whether the variety of service providers envisaged above will come within the definition of “preventative or counselling services” remains to be seen.

In this vein, therefore, it is recommended that consideration be given to defining “preventative or counselling services” for the purpose of the 2017 Bill. A broad definition should be applied to this phrase to ensure that the types of websites envisaged above fall within this exception to the general specialised protection envisaged for children by the GDPR. To ensure, therefore, that children’s access to information is not unreasonably restricted by blanket filters blocking websites which offer education and support, the legislature needs to define “preventative and counselling services” and it will be necessary to provide clarification on whether organisations that provide online support services to

children will have to verify the consent of the child's holder of parental responsibility before processing a child's data for not-for-profit use.

Holder of parental responsibility

It should be noted that Head 16 of the General Scheme of the 2017 Bill does not contain any definition of the phrase "the holder of parental responsibility over the child". This term is taken directly from the GDPR and has no clear meaning under Ireland's existing statutes concerning children. Clarification is thus required so that those persons who fall within this term are clearly identified. It is likely that the holder of parental responsibility will mean, for the purposes of Irish law, the child's parent or legal guardian. Given the recent expansion of the categories of person who may obtain guardianship in this jurisdiction and the court's power to limit the rights of certain non-parent guardians, merely defining a holder of parental responsibility as a "parent or guardian", may be inadequate and raise further queries. It is submitted therefore, that the "holder of parental responsibility" should include any parent and any guardian of the child, whether automatic or court appointed pursuant to the provisions of the Guardianship of Infants Act 1964, as amended by the Children and Family Relationships Act 2015. This would include temporary guardians, testamentary guardians and those appointed under s.6C of the 1964 Act. Applying a wide definition to this phrase is preferable to allow a broader category of persons who may be responsible for a child to be able to give the requisite consent for the child in question. It may ensure that children under 13 have a greater pool of persons from whom consent to sign up to digital services can be authorised.

A further concern with regard to the involvement of the "holder of parental responsibility" is that many parents or guardians of children have lower digital literacy skills compared with their child. Despite this, the GDPR places the responsibility to manage children's data protection on their parents and guardians where the child is under the digital age of consent. In this regard, in an Irish context, recent research compiled by DCU demonstrates that over half of parents expressed a frustrating lack of knowledge about privacy techniques, filtering and passport controls.[35] Such statistics are worrying. The consent of the data subject under the GDPR means "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".[36] To avoid a situation where parents or guardians are giving uninformed consent to the processing of their child's data, and to ensure that both children and their parents are equipped with the information necessary to make sound decisions on data protection issues, it is recommended that awareness needs to be raised in relation to the proposed digital age of consent, the meaning of data protection and processing, and the consequences of same. It appears that the Department of Justice and Equality recognises the need for such awareness-raising. In its Consultation Paper on *Data protection safeguards for children ("digital age of consent"),* published in November 2016, it noted that the GDPR requires that activities addressed to children must in future be given specific attention. It stated that this necessitates the development of appropriate child-friendly materials by the Data Protection Commission which "convey an understanding not only of

[35] Dublin City University, 'DCU research reveals digital divide between parents and children' <https://www.dcu.ie/news/2016/feb/s0216g.shtml> accessed 15 November 2016.

[36] Article 4(11) GDPR.

the risks that may arise when personal information is supplied online but also the remedies that are available under data protection law."[37] This is a welcome acknowledgment and I therefore recommend that the abovementioned efforts are taken to educate children and their parents on the importance of data protection alongside the progress of the 2017 Bill through the Oireachtas.

Right to be forgotten

In my ninth rapporteur report, I discussed the right to be forgotten and its importance from the perspective of a child.[38] The right to be forgotten was held to exist in the seminal case of *Google v Spain*.[39] In that decision, the European Court of Justice held that an EU citizen has the right to request that commercial search firms, such as Google, remove links to their personal information when requested, provided that the information is no longer relevant – emphasising an individual's right to privacy which overrides the public interest in access to information in certain circumstances. Article 17 of the GDPR concerns the "right to erasure", known as the right to be forgotten. It gives a data subject the right to obtain from the data controller the erasure of personal data concerning him or her, without undue delay. The controller is obliged to erase this personal data without undue delay where certain circumstances apply, for instance where the personal data is no longer necessary in relation to the purposes for which it was collected or processed; where it was processed unlawfully; or where the data subject withdraws consent on which the processing is based. There is no specific Head in the General Scheme that gives particular effect to Article 17 of the GDPR.

The right to be forgotten is not just an important right which may be exercised by adults. It is even more relevant for children. This is particularly so as children are less likely than adults to be aware that information they post online may be available long-term and they may not consider the consequences of posting something online which may last long beyond their childhood. The prevalence of social media and instant access to same through mobile technology compounds this problem. Given these considerable concerns, it is recommended that the age of the individual at the time of the digital posting of the information be a key factor in the exercise of the right to erasure. While not stated in Article 17 of the GDPR, it is suggested that Ireland should take the opportunity to include specific provisions on this issue in the 2017 Data Protection Bill. The relevance for children of the **"**right to be forgotten" should be acknowledged, children should be educated about the matter, and it should be understood that the age at which an individual posts information online should be considered a very important factor in decisions about whether to remove an individual's personal information from sites.

[37] Department of Justice and Equality, Data protection safeguards for children ('digital age of consent') Consultation Paper http://www.justice.ie/en/JELR/Consultation_paper_Digital_Age_of_Consent.pdf/Files/Consultation_paper_Digital_Age_of_Consent.pdf, at para 7.

[38] Geoffrey Shannon, *Ninth Report of the Special Rapporteur on Child Protection* (2016).

[39] *Google Spain, S.L., Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* ECLI:EU:C:2014:317.

Cyber-harassment and misuse of personal data

The GDPR and the General Scheme of the 2017 Bill cannot be considered in a vacuum. There are risks associated with young people maintaining an online presence which cannot be ignored. In this vein, the introduction of the Criminal Law (Sexual Offences) Act 2017 is to be welcomed and applauded. This Act demonstrates Ireland's commitment to better protecting its children from online predators and it specifically recognises the dangers that come with technological advances by creating a wide range of new criminal offences dealing with child pornography and grooming, with a particular emphasis on the use of information and communication technology in such offences. A further concern associated with children's internet usage is the prevalence of cyber-bullying or harassment. The prevalence of cyber-harassment is something which I considered in detail in my sixth rapporteur report.[40] The problem is widespread – one EU study indicated that 21% of children have been exposed to potentially harmful user-generated content such as hate, pro-anorexia and self-harm.[41] Where such problems are encountered, it is important to respond appropriately. Child development experts advise that parents should not restrict children's access to the internet, as it may prevent dialogue and discourage them from reporting abuse. Instead, supporting children with information about how to stay safe online, for example through changing privacy settings and reporting abuse, is advised. Furthermore, parents must be educated on this issue. The importance of dialogue and support for children, rather than simply imposing prohibitions on internet usage, should be part of this education.

In order to ensure that children are protected from cyber-bullying in their online activities and to ensure that their personal data is not exploited, regard should be had to the recommendation of the UN Committee on the Rights of the Child that States should "develop effective safeguards for children against abuse without unduly restricting the full enjoyment of their rights". It is notable that Article 6(2) of the GDPR enables Member States to "maintain or introduce more specific provisions to adapt the application of the rules…to ensure lawful and fair processing." This relates to data processing that is necessary for compliance with a legal obligation to which the data controller is subject or to processing that is necessary for the performance of a task carried out in the public interest. Having regard to Article 6(2) and the concerns raised above, I believe that further exploration is merited to ascertain whether these rules, or other mechanisms, could be used to enable the State to put specific legislative protection or exceptions in place to protect the right of children to participate online without having their data used for commercial gain.

To further address the issues raised above concerning cyber-harassment and bullying, I believe that regard should be had to the recommendations I have recently made in my tenth rapporteur report.[42] Online harassment is a reality in societies such as ours where people communicate regularly by e-mail and where social media platforms such as Facebook, Twitter and Instagram are used often. Such harassment can take a number of different forms. It may, for instance, involve the use of a fake Facebook profile to terrorise a victim through the publication of abusive material, images or videos about him or her which

[40] Geoffrey Shannon, *Sixth Report of the Special Rapporteur on Child Protection* (2013), at section 2.2.
[41] EU Kids Online network, available at: www.eukidsonline.net (last accessed 1 December 2015). Funded by the European Commission Safer Internet Programme (2009-11).
[42] Geoffrey Shannon, *Tenth Report of the Special Rapporteur on Child Protection* (2017), at section 2.2.

may be foul, fabricated, racist and/or defamatory. It could take place through the non-consensual publication of images online of an intimate nature, whether consensually generated or gained through covert recording. This type of publication often takes place out of spite or revenge, colloquially termed "revenge porn." In the alternative, the internet can be used to bully a particular person by the repetitive sending of nasty and malicious messages to the intended victim, often anonymously. The effects of these types of online behaviours are immediate, they have the capacity to go viral and they can be extremely invasive. Computers are not required to carry out a campaign of cyber-harassment as mobile devices are now equipped with the same internet options. This means that cyber-harassment can take place more frequently and with ease when perpetrated with the use of mobile phones. It enables perpetrators to communicate with others and disseminate content online instantly, with little effort.

Teenagers and young adults can be and often are targeted with such behaviour as outlined above. The prevalence of same has been recognised by An Garda Síochána with the publication of its Crime Prevention Information Sheet on Online Harassment (2012), directed towards both children and their parents. It cannot be denied that the capacity for damage from this type of harassment is enormous. Aside from the expected impact of such behaviour on a victim's emotional wellbeing, including embarrassment, hurt and fear, there can be other more drastic consequences of cyber-harassment, such as depression and suicide. Harassment or online abuse can equally have an impact on a young person's reputation and could potentially damage his or her future job opportunities.

Alongside recommendations that I made to address gaps in Ireland's existing criminal legislation in order to combat online harassment, I endorsed the recommendations of the Law Reform Commission in its 2016 Report on Harmful Communications and Digital Safety concerning "take down procedures" – a mechanism to ensure the efficient removal of harmful digital communications online.[43] The LRC, in its report, notes that the current non-statutory self-regulation by social media companies may not be sufficient to tackle harmful cyber communications. Drawing from experiences in Australia and New Zealand, the Commission proposes the establishment of a new statutory oversight system with a dual role of promoting digital safety and ensuring an efficient take down procedure for harmful digital communications. The proposed Office of the Digital Safety Commissioner of Ireland would therefore oversee an "effective and efficient" take down procedure in a timely manner, regulating for a system of take down orders in respect of harmful cyber communications made in respect of both adults and children. Its regulatory role would apply to a wide range of digital or online service providers, including any undertaking that provides a digital or online service, whether by the internet, a telecommunications system, the world wide web or otherwise. These are termed "digital service undertakings" and would include search engines, social media platforms and social media sites. The take down procedure would be made available to all affected individuals and would be free of charge.

Included in the role of the Digital Safety Commissioner would be to publish a Code of Practice on Take Down Procedures for Harmful Communications. The Code would give practical guidance on the take down procedure and set out the steps required by a digital

[43] LRC 116-2016 Report on Harmful Communications and Digital Safety.

service undertaking to meet National Digital Safety Standards. These standards would require a digital service undertaking to have in place a provision prohibiting the posting of harmful digital communications and to operate a complaints scheme to allow users to request the removal of such communications without charge. They also would set out a timeline for responding to complaints which must not be less stringent than that set out in the Code. The digital service undertaking would also be required to appoint a contact person to engage with the Commissioner. In essence, therefore, the take down procedure would first involve a complaint being made by the user directly to the digital service undertaking. If it did not remove the content or comply with the timeline specified in the Code, then the user could make a complaint to the Commissioner. At this point, the Commissioner would investigate the complaint and consider submissions from both the user and the digital service undertaking. If the Commissioner was satisfied that the undertaking had not complied with the Code or the National Digital Safety Standards, a determination could be made that the complaint be upheld and the undertaking would be directed to remove the harmful communication. The upholding of a complaint would result in the revocation of the undertaking's certificate of compliance. Failure to comply with the Commissioner's direction to take down the content, would entitle the Commissioner to apply to the Circuit Court for an order requiring compliance.

The proposal made by the Law Reform Commission regarding the establishment of a new statutory oversight system as detailed above appears to be a practical and viable solution to the current lacuna in the law, whereby take downs are difficult to achieve and civil remedies are often too expensive and ineffective. It is recommended therefore that consideration be given by the government to Chapter 3 of the Commission's Report forthwith, to enable progress to be made in this regard and to ensure that steps are taken to establish an Office of the Digital Safety Commissioner. It is further recommended, in light of the publication of the General Scheme of the 2017 Data Protection Bill that the Digital Safety Commissioner, if established, should be required to liaise with the Data Protection Commission operating pursuant to the 2017 Data Protection Bill. Cooperation between the two bodies would be essential to ensure that harmful communications are removed and potential breaches of data protection legislation investigated.

Processing of special categories of data

Article 9 of the GDPR concerns the processing of "special categories of personal data". It provides as follows:

> Processing of 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 shall be prohibited.[44]

Such processing, however, is permitted in a number of specified circumstances as set out in Article 9.2, including where the processing of such personal data is necessary for the provision of health or social care or treatment or the management of health or social care

[44] Article 9.1 GDPR.

systems and services,[45] subject to suitable and specific measures being implemented to safeguard the fundamental rights and freedoms of data subjects. In the General Scheme of the 2017 Bill, Heads 17 and 18 concern the processing of these special categories of data. Head 17 permits the making of regulations concerning the processing of sensitive data where "necessary for reasons of substantial interest", and Head 18, Sub-head 1 particularly provides that these categories of sensitive data may be processed where necessary for, inter alia, "the management of health and social care systems and services and for public interest reasons in the area of public health."

It can be imagined that the abovementioned exceptions to the prohibition of the processing of sensitive personal data will enable the Child and Family Agency (CFA) to process such data in the carrying out of its statutory role. This will inevitably include special sensitive data relating to children and young persons. The 2017 Bill only allows this processing to take place on the condition that suitable and specific measures are adhered to in order to safeguard the fundamental rights and interests of the data subject. As identified in the explanatory notes to Head 18, it is as of yet unclear as to the extent to which the "suitable and specific safeguards" referred to in Article 9 and included in the Bill are intended to be additional or complementary safeguards to those already placed upon data controllers elsewhere in the GDPR or whether additional safeguards will be required. Given the nature of the data involved, it is recommended that consideration be given to the inclusion of additional safeguards, particularly where a child's sensitive personal data is engaged and is to be processed by the CFA. This should be explored having regard to Recital 38 of the GDPR and the special protection required therein for the personal data of children.

Dr. Geoffrey Shannon
28 June 2017

[45] Article 9.2(h).

Appendix 5 - Submission by Dr Eoin O'Dell

Submission on the General Scheme of the Data Protection Bill 2017 to the Committee on Justice and Equality

by Dr Eoin O'Dell[*]

1. Introduction

In the European Union, the Charter of Fundamental Rights guarantees the right to respect for private life, in general, and to the protection of personal data, in particular.[1] The Court of Justice of the European Union has long stressed the importance of these rights;[2] the Charter has added impetus to their recognition and protection;[3] and they are given detailed effect by the General Data Protection Regulation.[4] Rights require remedies, and the GDPR provides a strong regime of regulation and sanctions. Public regulation and enforcement are undertaken by national data protection supervisory authorities, such as the Office of the Data Protection Commissioner. However, private enforcement is a significant part of the GDPR; hence, to give effect to the right to an effective judicial remedy in accordance with Article 47 of the Charter,[5] data subjects can claim compensation from controllers or processors for damage suffered as a result of processing that infringes the GDPR. In particular, Article 82(1) GDPR provides:

---

[*] Fellow and Associate Professor of Law

[1] See Articles 7 and 8 of the Charter Fundamental Rights of the European Union [hereafter: CFR]. See also Article 16(1) of the Treaty on the Functioning of the European Union [hereafter: TFEU] (right to the protection of personal data).

[2] Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof v Österreichischer Rundfunk* (ECLI:EU:C:2003:294; ECJ, 20 May 2003) [68], [73]-[75]; Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España* [2008] ECR I-271 (ECLI:EU:C:2008:54; ECJ, 29 January 2008) [63].

[3] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* (EU:C:2010:662; CJEU, 9 November 2010) [47]; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (ECLI:EU:C:2014:238; CJEU, 8 April 2014) [29], [40]; Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos* (ECLI:EU:C:2014:317; CJEU, 13 May 2014) [69]; C-212/13 *Ryneš v v Úřad pro ochranu osobních údajů* (ECLI:EU:C:2014:2428; CJEU, 11 December 2014) [28]-[29]; Case C-230/14 *Weltimmo sro v Nemzeti Adatvédelmi és Információszabadság Hatóság* (ECLI:EU:C:2015:639; CJEU, 01 October 2015) [25], [30]; Case C-362/14 *Schrems v Data Protection Commissioner* (ECLI:EU:C:2015:650; CJEU, 6 October 2015) [37]-[40].

[4] Regulation 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 [the General Data Protection Regulation; hereafter: GDPR]; it will apply from 25 May 2018 (see Article 99(2) GDPR).

[5] See Case C-362/14 *Schrems v Data Protection Commissioner* (ECLI:EU:C:2015:650; CJEU, 6 October 2015) [95] (effective judicial remedy necessary to vindicate privacy and data protection rights); see also Article 19 of the Treaty on the European Union (Member States' duty to provide remedies sufficient to ensure effective legal protection in the fields covered by EU law).

> Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. …

As a consequence, compliance with the GDPR is ensured through a mutually reinforcing combination of public and private enforcement that blends public fines with private damages. In particular, claims for compensation pursuant to Article 82 GDPR strengthen the working of the Regulation, since they discourage practices, frequently covert, which are liable to infringe the rights of data subjects, thereby making a significant contribution to the protection of privacy and data protection rights in the European Union.[6]

Legislation is necessary to give further effect to the GDPR in Irish law, and this is provided for in the General Scheme of the Data Protection Bill 2017.[7] Head 91 of the Scheme provides "a data protection action" to data subjects whose rights under the GDPR or its translating legislation are infringed.[8]

The Police and Criminal Justice Authorities Directive[9] was adopted alongside the GDPR, and it also provides for both public and private enforcement, including a claim for compensation. Article 56 PCJAD provides:

> Member States shall provide for any person who has suffered material or non-material damage as a result of an unlawful processing operation or of any act infringing national provisions adopted pursuant to this Directive to have the right to receive compensation for the damage suffered from the controller or any other authority competent under Member State law.

Head 58 of the Scheme provides a claim for compensation to any person whose rights under the Part of the Scheme transposing the PCJAD have been infringed.[10]

A claim for compensation in a Regulation is unusual but not unique as a matter of EU law.[11] On the other hand, a claim for compensation in a Directive, such as the PCJAD,

---

6 See, by analogy, the approach of the CJEU to the private enforcement of EU competition rules: Case C-557/12 *Kone AG v ÖBB-Infrastruktur AG* (ECLI:EU:C:2014:1317; CJEU, 5 June 2014) [23].

7 Hereafter: the Scheme.

8 Head 91 is set out in Part 1 of the Appendix, below.

9 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 [The Police and Criminal Justice Authorities Directive; hereafter: PCJAD]; this will have to be implemented before 6 May 2018 (see Article 63(1) PCJAD).

10 Head 58 is set out in Part 1 of the Appendix, below.

is quite common as a matter of EU law.[12] In either case, the formulations of such claims are usually clear. However, the formulation in Article 82(1) GDPR. It does not say that a person whose rights have been infringed *has* the right to receive compensation. Instead, it provides, in a much more mealy-mouthed fashion, that a plaintiff *shall have* such a right. Whilst this is similar to Article 5(1)(c) of the Flight Cancellation Regulation, there is no further phrase like Article 7 of that Regulation, which provides additionally and unambiguously that "passengers *shall receive* compensation". The mandate in Article 82(1) GDPR that plaintiffs "shall have" a claim seems to imply that there is something more to be done in national law before plaintiffs actually have the claim. Admittedly, this does not replicate any of the usual strictures in a Directive, found for example in Article 56 PCJAD, that Member States shall "provide" or "ensure" or "introduce" or "lay down" measures to achieve an outcome, such as a claim for compensation. But the formulation in Article 82(1) GDPR still seems to envisage some national law mechanism in ensuring that a plaintiff "shall" have a claim to compensation. It does not seem to be sufficiently clear, precise and unconditional to create a direct horizontal claim for compensation that can be relied upon in the Irish courts without an express provision giving effect to it in the Scheme.

On the other hand, the CJEU has provided expansive interpretations of claims for compensation pursuant to various other Regulations[13] and Directives,[14] A similarly expansive interpretations of the claim for compensation for damage in Article 82(1) GDPR is inevitable, not least because Recital 146 GDPR provides:

---

[11] Regulation (EC) No 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No 295/91 [hereafter: the Flight Cancellation Regulation]; Council Regulation (EC) No 2100/94 of 27 July 1994 on Community plant variety rights [hereafter: the Plant Variety Rights Regulation], given full effect by the European Communities (Protection of Plant Variety Rights) Regulations 2007 (SI No 273 of 2007).

[12] See, *eg*, Folkert Wilman *Private Enforcement of EU Law Before National Courts: The EU Legislative Framework* (Edward Elgar, Cheltenham, 2015). Directives provide claims for compensation for defective products, infringements of package holiday contracts, public procurement rules, intellectual property rights, competition law, trade secrets, and equality.

[13] Case C-481/14 *Hansson v Jungpflanzen Grünewald GmbH* (ECLI:EU:C:2016:419; CJEU, 9 June 2016) [Plant Variety Rights Regulation]; Joined Cases C-402/07 and C-432/07 *Sturgeon v Condor Flugdienst GmbH and Böck v Air France SA* [2009] ECR-I 10932 (ECLI:EU:C:2009:716; CJEU, 9 November 2009) [Flight Compensation Regulation].

[14] Case C-271/91 *Marshall v Southampton and South-West Hampshire Area Health Authority* [1993] ECR I-04367 (ECLI:EU:C:1993:335; ECJ, 2 August 1993) (compensation must enable the loss and damage actually sustained to be made good in full); Case C-168/00 *Leitner v TUI Deutschland GmbH* [2002] ECR 1-1631 (ECLI:EU:C:2002:163; ECJ, 12 March 2002) (claim for compensation includes non-material damage, such as distress); Case C-314/09 *Stadt Graz v Strabag AG* [2010] ECR I-8769 (ECLI:EU:C:2010:567; ECJ, 30 September 2010) (claim for compensation not conditional on fault)

> … The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. … Data subjects should receive full and effective compensation for the damage they have suffered. …

However, such an expansive interpretation by the CJEU is inevitable *only if it is asked*; and, unless and until it is, there is the potential for great uncertainty. It would therefore be better to have this matter settled by legislation rather than leaving it to the vagaries of litigation to – and in – the CJEU. The clearest solution would be to provide expressly for a claim for compensation in the Scheme, just as an express claim to compensation is necessary to transpose Article 56 PCJAD.

Where such legislation is necessary, then a failure to enact it could leave the State open to a claim for damages from someone who suffered loss by reason of the State's failure to give full effect to Article 82(1) GDPR.[15]

For all of these reasons, therefore, the Scheme giving full effect to the GDPR and transposing the PCJAD into Irish law should expressly provide for the claims for compensation in Article 82(1) GDPR and Article 56 PCJAD. Heads 91 and 58 (respectively) of the Scheme address this issue, but they do not successfully provide for such claims for compensation.

Article 79 GDPR provides for a right to an effective judicial remedy against a controller or processor; and Article 82 GDPR provides for a claim for compensation as part of that effective judicial remedy. Head 91 of the Scheme seems to be directed towards these Articles.[16] Head 91(1) provides what it describes as "a data protection action" to data subjects whose rights under the GDPR or its translating legislation are infringed. Head 91(2) provides jurisdiction to the Circuit Court, concurrently with the High Court, to hear such actions. Head 91(3) provides:

> 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.

And Head 91(4)(b) requires a plaintiff in a data protection action to specify, *inter alia*, "any material or non-material damage alleged to have been occasioned by the infringement".

---

[15] Joined cases C-178/94, C-179/94, C-188/94, C-189/94 and C-190/94 *Dillenkofer v Germany* [1996] ECR I-4845 (ECLI:EU:C:1996:375; ECJ, 8 October 1996) (Germany's failure to transpose the original Package Holidays Directive gave rise to a claim for damages for holiday-makers who failed to get compensation and refunds for holidays where the organizers became insolvent).

[16] Head 91 is set out in Part 1 of the Appendix, below.

The reference in Head 91(3) to the provision of other remedies "without prejudice to [the Circuit Court's] … powers to award compensation" assumes that the Court has such powers. And the reference in Head 91(4)(b) to "any material or non-material damage" further assumes that that the powers to award compensation cover both material and non-material damage. However, Head 91 does not expressly afford a claim compensation for material or non-material damage; nor is it expressly afforded elsewhere in the Scheme. It may be that this Head is predicated on the assumption that Article 82(1) GDPR is directly horizontally effective and thereby provides those "powers to award compensation. However, for the various reasons set out above, it is not so clear that Article 82(1) GDPR is indeed directly horizontally effective. Whilst Head 91 provides a superstructure for an effective judicial remedy for infringement of the GDPR or of its translating legislation, and whilst it assumes a claim for compensation, it does not expressly provide one. Rather than hope that litigation to the CJEU establishes that Article 82(1) GDPR is directly horizontally effective and requires that it be interpreted expansively, the best solution would be for Head 91 of to contain an express provision giving full effect to Article 82(1) GDPR in Irish law.

The architecture of the PCJAD in this respect is very similar to the GDPR. Article 54 PCJAD provides for a right to an effective judicial remedy against a controller or processor; and Article 56 PCJAD provides for a claim for compensation as part of that effective judicial remedy. Head 58 of the Scheme seems to be directed towards these Articles.[17] It provides that a person "who suffers material or non-material damage" by reason of an infringement of the Part of the Scheme transposing the PCJAD "shall have the right to receive compensation …". This is a clear claim for compensation, and it is unfortunate that a similarly clear clause was not provided in Head 91. However, Head 58 does not locate this claim for compensation in a superstructure for an effective judicial remedy for infringement of that Part of the Scheme, comparable with the superstructure provided in Head 91. It may be that Head 58 is predicated on the assumption that ordinary court procedures will fill that gap. Rather than hope that litigation will work this issue out, the best solution would be for the claim for compensation in Head 58 of the Scheme to be contained an express superstructure for an effective judicial remedy, much as is provided in Head 91.

Both Head 58 and Head 91 do half the necessary work, and each does a different half: whereas Head 58 contains an express claim for compensation but does not provide a superstructure for an effective remedy, Head 91 provides a superstructure for an effective remedy but does not contain an express claim for compensation. The

[17] Head 58 is set out in Part 1 of the Appendix, below.

solution is simple; in Head 58, add a superstructure for an effective remedy along the lines of that already provided in Head 91; and, in Head 91, add an express claim for compensation, following the lead of Head 58. In this way, the issues of compensation and remedies for infringement of the GDPR and the PCJAD can be dealt with on a consistent basis in the Scheme.

In amending these Heads, three principles should be borne in mind. First, the claim for compensation should commence with as much of the language as possible of Article 82(1) GDPR and Article 56 PCJAD. In this context, a decision will have to be made as to whether the legislation should follow the lead of the Regulations and refer to "compensation" for their breach, or whether it should follow normal Irish practice and refer to "damages". Given that "compensation" in EU terms can be taken to mean "damages" in Irish terms, translating or transposing legislation should refer to "damages" where the relevant Regulations or Directives refer to "compensation". Nothing will be lost in translation or transposition, and accuracy of analysis at Irish law will be gained.

Head 91 of the Scheme begins, but does not complete, the process of giving full effect to Article 82 GDPR in Irish law. In particular, while it provides a superstructure for an effective judicial remedy for infringement of the GDPR or of the Scheme it does not contain an express claim for compensation. It should therefore be amended to include a new subsection using as much of the language of Article 82(1) GDPR as possible, modified to refer to damages rather than compensation.[18]

Similarly, Head 58 of the Scheme begins, but does not complete, the process of transposing Article 56 PCJAD into Irish law. In particular, while it contains an express claim for compensation, it does not provide a superstructure for an effective judicial remedy for infringement of the Part of the Scheme transposing the PCJAD. The claim for compensation in Head 58 could be improved if it cleaved even more closely to the language of Article 56 PCJAD, modified to refer to damages rather than compensation. And that Head should be further amended to locate this claim for damages in the context of a superstructure for an effective judicial remedy, comparable with the superstructure provided in Head 91.[19]

The second principle to be borne in mind is that the nature of the damages claim at national law will have to be clarified. For example, in giving effect to Article 1 of the Products Liability Directive, section 2(1) of the Liability for Defective Products Act, 1991 characterised the claim as one for "damages in tort". Again, the Sea Pollution

[18] See the draft of Head 91(2) in Parts 2 and 3 of the Appendix, below.

[19] See the draft of Head 58(1), (3)-(6) in Parts 2 and 3 of the Appendix, below.

(Hazardous Substances) (Compensation) Act 2005 gives effect to the International Convention on Liability and Compensation for Damage in connection with the Carriage of Hazardous and Noxious Substances by Sea, 1996. Section 16(1) of that Act provides:

> An action for compensation under the Convention … shall be deemed for the purposes of every enactment and rule of law to be an action founded on tort.[20]

If a provision equivalent to section 16(1) were included in Heads 58 and 91 of the Scheme, then fundamental legal issues such as causation, remoteness, measures of damages (including disgorgement, and aggravated, and exemplary or punitive, damages), mitigation, limitation, contributory negligence, vicarious liability, defences, damages jurisdictions in the various courts, and so on, could be resolved by the application of settled principles of tort law. These claims would then be equivalent to, and thus not less favourable than, those relating to similar domestic claims; and they would be effective and thus not virtually impossible or excessively difficult to employ.

However, there is no provision equivalent to section 16(1) of the 2005 Act in Heads 58 or 91 of the Scheme; so it should be expressly provided that the claims in Heads 58 and 91 "shall be deemed for the purposes of every enactment and rule of law to be an action founded on tort".[21] Furthermore, such an express reference to tort would reinforce the proposal above that the translating and transposing legislation should refer to "damages" where Article 82(1) GDPR, and Article 56 PCJAD refer to "compensation".

The second principle to be borne in mind is that Head 91 should be as comprehensive as possible in giving effect to Article 82 GDPR, and that Head 58 should be as comprehensive as possible in transposing Article 56 PCJAD. In particular, if a provision modelled on Article 82(1) GDPR is to be added to Head 91 of the Scheme, then other elements of Article 82 may also need be added. On the one hand, Article 82(4) and (5) GDPR provide for concurrent, and joint and several, liability. If a provision is added to Head 91 providing that the data protection claim in that Head is an action founded on tort, then the provisions of Part III of the Civil Liability Act, 1961 will deal with issues of concurrent, and joint and several, liability; and it will not be necessary to give further effect to 82(4) and (5) GDPR. On the other

---

[20] Section 28 of the Merchant Shipping (Liability of Shipowners and Others) Act, 1996 is to similar effect. See also section 32(6) of the Competition Act 2002 and section 32(7) of the Consumer Protection Act 2007, unaccountably not re-enacted in section 25 of the Competition and Consumer Protection Act 2014.

[21] See the drafts of Heads 58(7) and 91(7) in Parts 2 and 3 of the Appendix, below.

hand, Article 82(2) and (3) provide for some defences to the claim for compensation in Article 82(1), and if the claim in Article 82(1) is added to Head 91, then the defences to the claim will have to be added to Head 91 as well.[22]

Claims for compensation are an important part of the enforcement architecture of the GDPR, of its associated PCJAD, and of the Scheme. Given that some of the choices in the Scheme have the effect of limiting public enforcement,[23] private enforcement mechanisms become crucial. They will help to discourage infringements of the rights of data subjects; they will make a significant contribution to the protection of privacy and data protection rights in the European Union; and they will help to ensure that the great promise of the GDPR is fully realised.

[22] See the draft of Head 91(8) in Parts 2 and 3 of the Appendix, below; and see the impact on the draft of Head 58(8) in Parts 2 and 3 of the Appendix, below.

[23] For example, Head 23 of the Scheme envisages that administrative fines may be imposed on public authorities and bodies for breaches of the GDPR and its translating legislation arising in the course of the provision of goods or services for gain but not in the course of the provision of their public functions.

Appendix

1. Heads 58 and 91 of the General Scheme of the Data Protection Bill 2017

Head 58 – Right to compensation

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.

Head 91 – Judicial remedy

(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 alleged controller or processor is a public authority of the State acting in the exercise of its public powers.

2. Suggested amendments to Heads 58 and 91

Suggested additions **appear thus**; suggested deletions ~~**appear thus**~~

Head 58 – ~~**Right to compensation**~~ **Judicial remedy and damages**

(1) Where a person considers that his or her rights have been infringed as a result of an unlawful processing operation or other act infringing this Part, then such unlawful processing or other infringement shall be actionable at the suit of the person concerned ("infringement action").

(2) In an infringement action under this Head, a ~~A~~ person **who has suffered ~~suffers~~ material or non-material damage as a result of ~~by reason of~~** an infringement of this Part shall have the right to receive ~~**compensation**~~ **damages** from the competent authority or processor for **the** damage ~~**or distress**~~ suffered.

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

(4) In an infringement action under this Head, the Circuit Court shall, without prejudice to its powers to award damages pursuant to sub-Head (2), also have the power to grant relief by means of injunction or declaratory orders.

(5) For the purpose of commencing an infringement action, the plaintiff shall, in particular, specify—

(a) particulars of the acts of the competent authority or processor constituting the alleged unlawful processing or other infringement, and

(b) any material or non-material damage alleged to have been occasioned by the alleged unlawful processing or other infringement.

(6) The jurisdiction conferred on the Circuit Court by this Head may be exercised by the judge of the circuit in which—

(a) the competent authority or processor has an establishment, or

(b) the data subject has his or her habitual residence except where the competent authority or processor is a public authority of the State acting in the exercise of its public powers.

(7) An infringement action under this Head shall be deemed for the purposes of every enactment and rule of law to be an action founded on tort.

(8) In an infringement action under this Head, it shall be a defence for a competent authority or processor to show that it is not in any way responsible for the event giving rise to the alleged damage.

Head 91 – Judicial remedy **and damages**

(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) In a data protection action under this Head, a data subject who has suffered material or non-material damage as a result of an infringement of the Regulation or this Act shall have the right to receive damages from the controller or processor for the damage suffered.

(3)~~(2)~~ The Circuit Court shall, concurrently with the High Court, have jurisdiction to hear and determine proceedings **in data protection actions** under this Head.

(4)~~(3)~~ In a data protection action under this Head, the Circuit Court shall, without prejudice to its powers to award **damages pursuant to sub-Head (2), also ~~compensation in respect of material or non-material damage,~~** have the power to grant relief by means of injunction or declaratory orders.

(5)~~(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 **alleged** infringement.

(6)~~**(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.

(7) A data protection action under this Head shall be deemed for the purposes of every enactment and rule of law to be an action founded on tort.

(8) (a) Without prejudice to its liability as a controller, any controller involved in processing shall also be liable in a data protection action under this Head for the damage caused by processing which infringes the Regulation or this Act.

(b) A processor shall be liable in a data protection action under this Head for the damage caused by processing only where it has not complied with obligations of the Regulation or this Act specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

(c) In a data protection action under this Head, it shall be a defence for a controller or processor to show that it is not in any way responsible for the event giving rise to the alleged damage.

3. Heads 58 and 91 after suggested amendment

Head 58 – Judicial remedy and damages

(1) Where a person considers that his or her rights have been infringed as a result of an unlawful processing operation or other act infringing this Part, then such unlawful processing or other infringement shall be actionable at the suit of the person concerned ("infringement action").

(2) In an infringement action under this Head, a person who has suffered material or non-material damage as a result of an infringement of this Part shall have the right to receive damages from the competent authority or processor for the damage suffered.

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

(4) In an infringement action under this Head, the Circuit Court shall, without prejudice to its powers to award damages pursuant to sub-Head (2), also have the power to grant relief by means of injunction or declaratory orders.

(5) For the purpose of commencing an infringement action, the plaintiff shall, in particular, specify—

(a) particulars of the acts of the competent authority or processor constituting the alleged unlawful processing or other infringement, and

(b) any material or non-material damage alleged to have been occasioned by the alleged unlawful processing or other infringement.

(6) The jurisdiction conferred on the Circuit Court by this Head may be exercised by the judge of the circuit in which—
  (a) the competent authority or processor has an establishment, or
  (b) the data subject has his or her habitual residence except where the competent authority or processor is a public authority of the State acting in the exercise of its public powers.

(7) An infringement action under this Head shall be deemed for the purposes of every enactment and rule of law to be an action founded on tort.

(8) In an infringement action under this Head, it shall be a defence for a competent authority or processor to show that it is not in any way responsible for the event giving rise to the alleged damage.

Head 91 – Judicial remedy and damages

(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) In a data protection action under this Head, a data subject who has suffered material or non-material damage as a result of an infringement of the Regulation or this Act shall have the right to receive damages from the controller or processor for the damage suffered.

(3) The Circuit Court shall, concurrently with the High Court, have jurisdiction to hear and determine proceedings in data protection actions under this Head.

(4) In a data protection action under this Head, the Circuit Court shall, without prejudice to its powers to award damages pursuant to sub-Head (2), also have the power to grant relief by means of injunction or declaratory orders.

(5) 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 alleged infringement.

(6) 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.

(7) A data protection action under this Head shall be deemed for the purposes of every enactment and rule of law to be an action founded on tort.

(8) (a) Without prejudice to its liability as a controller, any controller involved in processing shall also be liable in a data protection action under this Head for the damage caused by processing which infringes the Regulation or this Act.

(b) A processor shall be liable in a data protection action under this Head for the damage caused by processing only where it has not complied with obligations of the Regulation or this Act specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

(c) In a data protection action under this Head, it shall be a defence for a controller or processor to show that it is not in any way responsible for the event giving rise to the alleged damage.

Appendix 6 – Submission by IBEC

1. Digital development is important to economic growth and jobs

The use of digital technologies and data can be leveraged to enhance efficiencies in our infrastructure[1], in public administration for citizens[2] and enable business to compete, invest, grow and create jobs. Economically, digital technology can boost productivity and reduce transaction and information costs[3].

Data processing is now an integral part of companies' operations and trades. The success of our economy's ongoing digital transformation and our global competitiveness depends on the ability of businesses to process data both within and across our borders – enabling businesses to connect, innovate, develop, trade and meet their customers' requirements. The ongoing transformation of the European internal market into a "data-driven economy" is becoming critical to every sector, including financial services, business services, retail, energy, healthcare, agri-foods, manufacturing, logistics, transport, telecommunications, technology and more – our members are already investing in this transformation. Small and Medium sized Enterprises (SMEs) have an enormous potential for employing digital technologies to boost their productivity, access new markets and grow - creating new ecosystems and jobs[4] [5] [6]. While there is more progress to be made, the European Commission rank Ireland above the EU average for both the integration of digital technology by business and SME engagement in e-commerce[7]. SMEs represent 52.1% of Ireland's GDP[8] and employ 65% of the private sector workforce[9].

The European Commission is midway through the implementation of its digital single market (DSM) strategy[10]. An effective DSM framework could create up to €415 billion in additional growth to Europe's economy – both by enhancing the existing single market and as a potential vehicle that enables trade in the global digital marketplace. Ireland and other northern European 'digital frontrunners'[11] have been identified as countries that could benefit from an accelerated development of the European digital economy[12]. For Ireland the DSM and full adoption of digital technologies could be leveraged to add €27 billion to our GDP and have a positive net effect of up to 140,000 jobs by 2020[13].

Ireland's digital economy is estimated to be worth 6% of GDP or €12.3 billion – a value that has increased 39.3% in the period 2012-2015. The digital economy is estimated to be 5.7% of EU GDP and 5.3% of G20 GDP[14]. Ireland has a strong tradition and success in attracting global digital companies and developing a growing indigenous technology sector[15]. This

[1] Digital and data can be used to complement broader policy decisions and enhance efficiencies in our transport, energy, education and health systems https://ec.europa.eu/digital-agenda/en/smart-cities.
[2] European Parliament Research Service (2015) The use of digital by public bodies can reduce costs of public administration by 15-20%. A digital by default strategy in the public sector in the EU could result in around €10 billion of annual savings. http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/565890/EPRS_IDA(2015)565890_EN.pdf
[3] World Bank (2016) World Development Report 2016 – Digital Dividends; and World Economic Forum – WEF (2015) The global information technology report.
[4] DCENR (2016) Growing small business through online trade – enterprise impacts of the trading online voucher scheme.
[5] Accenture (2017) https://www.accenture.com/ie-en/company-ireland-as-a-startup-island
[6] Silicon Republic (2017) https://www.siliconrepublic.com/start-ups/google-adopt-a-start-up
[7] European Commission (2017) Digital Economy and Society Index (DESI) – Ireland. The DESI composite index summarises indicators on Europe's digital performance and tracks the evolution of EU member states in digital competitiveness https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2017
[8] SFA (2016) http://www.sfa.ie/Sectors/SFA/SFA.nsf/vPages/News~next-generation-business---a-vision-for-small-firms-in-ireland-30-05-2016/$file/SFA+Vision_Next+Generation+Business.pdf
[9] CSO- Business Demography Survey
[10] European Commission (2017) Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy COM(2017) 228 final
[11] Ireland, the Benelux countries, Denmark, Sweden, Finland, Norway and Estonia have been identified as digital front-runners. The frontrunners typically have relatively small populations and are well digitized, innovative and export driven.
[12] BCG (2016) Digitizing Ireland – How Ireland can drive and benefit from an accelerated digitized economy in Europe
[13] BCG (2016) Digitizing Europe – Why Northern European frontrunners must drive digitization of the EU economy
[14] DCCAE (2016) Assessment of the macro-economic impact of the internet/digital on the Irish economy, commissioned by the Department of Communications, Climate Action and Environment and prepared by Indecon.
[15] IDA (2017) http://www.idaireland.com/business-in-ireland/industry-sectors/ict/

success could leverage new investment in emerging technology strands and the creation of new cross-sectoral digital ecosystems.

2. Data protection matters in growing our digital economy

The European institutions believe that innovation, trust and security are core elements in building a robust digital single market and inclusive digital society. The recent reform of EU rules on data protection not only aim to protect the rights of individuals but aim to harmonise rules on data protection across the EU – avoiding fragmentation or legal uncertainty in a digital single market and building trust and inclusion for both business and citizens in that market. A harmonised and workable EU data protection framework, which balances privacy, security and innovation concerns, is important to delivering a European digital single market that provides growth and jobs for EU citizens.

3. Legal certainty is important in our growing our digital economy

3 (A) REGULATORY CERTAINTY

There is roughly 11 months before a new EU data protection framework applies on 25 May, 2018 – time is tight and our members are already preparing for compliance. The upcoming Data Protection Bill is an important milestone for preparing for May 2018. Implementation of the updated EU rules will involve interplay between:

- The direct effect of the EU General Data Protection Regulation, EU 2016/679 (GDPR) at Member State level.
- Transposition of certain GDPR elements and the Directive (EU 2016/680) across the Member States e.g. the upcoming Irish Data Protection Bill **(DP Bill**).
- Guidance from individual data protection supervisory authorities across Member States, and guidance from the Article 29 working party (consisting of representatives of the data protection supervisory authorities from the EU Member States and EU institutions) – soon to be the future decision-making role of the European Data Protection Board.
- The interplay between the GDPR and the European Commission's recently proposed ePrivacy Regulation (EPR).
- Evolving case law of the European Court of Justice.

In this context:

- Excepting the Data Protection Bill provisions which seek to implement the Law Enforcement Directive, we highlight the need to limit the provisions of the DP Bill to those which are essential to (a) implement derogations or adopt enabling measures permitted or required by the GDPR and (b) put in place the administrative machinery necessary for the Irish supervisory authority, the Data Protection Commission (the **Commission** or **DPC)** to exercise the powers conferred on it by the GDPR. Any provisions which go further than this risk creating an uneven data protection landscape across the EU. Further provisions would also contradict the purpose of data protection legislation being passed as a Regulation and not as a Directive in order to avoid the fragmentation in the implementation of data protection rules across the EU, legal uncertainty and differences in the level of protection of the rights and freedoms of data subjects.
- Our preference is that the new Irish legal instrument provides certainty for organisations seeking to comply with the updated rules both in Ireland and across the digital single market. As noted in the testimony at the Joint Committee's debate on 14

June, ‘there is no guarantee presented in the Heads of Bill that were published that the existing Irish Data Protection Acts 1988 and 2003 will be repealed’. It was suggested that a ‘patchwork presentation’ of law could potentially lead to legal uncertainty. To promote certainty, the new DP Bill should provide a single one-stop-shop for Irish law on data protection. Our preference is for the repeal of the Data Protection Acts 1988 and 2003. We agree with the Data Protection Commissioner that any provisions of the 1988 and 2003 Acts which need to be retained could be readily identified and included in a new stand-alone modernised Bill.

- The inevitable uncertainty that can result from principles-based legislation is a concern to Irish employers, particularly in circumstances where significant fines can be imposed and individuals can claim compensation for both material and non-material damage. Ibec, therefore, welcome the guidance provided to date by the data protection supervisory authorities and ask that they continue their engagement with business on guidance around aspects of the GDPR.
- We ask that the Irish government continue to work with EU partners to align the proposed ePrivacy Regulation (EPR) with the General Data Protection Regulation and not disrupt the current balance between protecting personal data and facilitating innovative business models. The proposed EPR is broad in scope and many of its provisions refer or relate to other EU legislation under discussion or yet to be implemented e.g. the GDPR, which organisations and supervisory authorities are preparing to implement by May 2018. To ensure a coherent regulatory framework, the EPR should align and complement other EU legislation and not undermine regulatory certainty or investment made in anticipation of GDPR implementation. Quality should take priority over speed in this process. Sufficient time is needed by the co-legislators to fully consider and improve the EPR proposal. Stakeholders who will apply the final result should also receive sufficient time to prepare.
- We submit that the Department of Justice and Equality should undertake a Regulatory Impact Assessment (RIA) to analyse the potential economic and social impact of the proposals contained in the general scheme, particularly with respect to those proposed provisions which are not mandated by the GDPR.
- There are a number of aspects of the general scheme which require further clarification and detail in order to provide the level of precision and certainty required to enable businesses and employers to properly comply with its provisions. Ibec also believes that the general scheme would benefit from additional rigour in areas which are currently left to the discretion of individual officers. Ibec will, therefore, also provide a more detailed submission to the Department of Justice and Equality in this regard.

3 (B) CONFIDENTIALITY OF INVESTIGATIONS (HEADS 14 & 85)

We are concerned about the confidentiality of information that may be required to be disclosed to the DPC in the course of an investigation/audit, and note that there is a requirement under Article 54(2) of the GDPR for the DPC and its staff to be subject to a duty of professional secrecy during and after their term of office.

We note that staff of the Commission will (as civil servants), be required under the Official Secrets Act 1963, to avoid unlawful communication of information gained in the course of their official work (see Head 10). Head 14(1) of the DP Bill contains a prohibition against the disclosure of information that comes into the DPC's possession. Firstly, this prohibition is narrower than the duty of professional secrecy required by Article 54 of the GDPR. A duty of professional secrecy would for example, cover any unauthorised use of confidential information (in addition to a prohibition on disclosure).

There is, therefore, merit in clarifying that Head 14 prevents, unless authorised or obliged by law to do so, the disclosure of confidential information, or the use, for the direct or indirect

advantage of themselves or another, of confidential information obtained in the course of carrying out one's functions/powers. This would ensure both the disclosure and improper use of the confidential information is restricted.

Secondly, we believe that the exceptions to the duty of confidence should be narrowed. Disclosure should only be permitted where it is required by law or it is strictly necessary for the performance of a particular statutory duty by the DPC. The disclosure of information may in many cases put at risk rights such as intellectual property or trade secrets. This justifies the need to implement narrow exceptions that allow for the adequate protection of the relevant rights at stake.

In addition, a lack of clarity and overly broad exceptions to the prohibition on disclosure of information could undermine companies' confidence in providing information which may be necessary for the Commission to have a full view of the issues to be considered. For example, the scope of the exception at Head 14(2)(b) is unclear as to whether it could extend to a discovery order. There has to be a reasonable degree of protection for commercially sensitive information and information submitted in confidence to enable a proper relationship of trust between companies and the Commission.

Thirdly, Head 14 is not immediately reconcilable with the efforts of the Commission to publicise complaints or investigations, to the extent that such publications could disclose any confidential information. Head 85 places an obligation on the DPC to publish particulars about any conviction/corrective action and confers discretion on the DPC to publish particulars of any report or investigation or audit carried out by the DPC. Heads 14 and 85 need to make it clear that the DPC cannot publish certain categories of information. As mentioned above the Commission may, for example, be privy to a lot of financial, commercial, scientific and technical information, trade secrets and other confidential information in the course of investigations the publication of which has the potential to irreversibly damage a business. We suggest that the following subhead is added to Head 85 as Head 85(5):

> ***"5. Nothing in this section 85 shall permit publication by the Commission of:***
>
> ***(a) confidential information, trade secrets, or any other particulars that may be***
> ***subject to the intellectual property rights of a person,***
> ***(b) financial, commercial, scientific or technical or other information whose disclosure could reasonably be expected to result in a financial loss or gain to the***
> ***person to whom the information relates, or could prejudice the competitive position of that person in the conduct of his or her profession or business or otherwise in his or her occupation, or***
> ***(c) information whose disclosure could prejudice the conduct or outcome of contractual or other negotiations of the person to whom the information relates."***

We also submit that publication of corrective measures should not be published where for example de minimis fines/fines below specified thresholds are imposed or there is no public interest in publication.

We have set out proposed amendments to Head 14:

> *"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. Except as otherwise provided or authorised by this section or another enactment, a person shall not, unless authorised or obliged by law to do so, disclose information, or use, to the direct or indirect advantage of himself or herself or of another person (other than the DPC), information that he or she obtained—

(a) while a member of the Commission,
(b) while an officer of the Commission or a staff member of the Commission or otherwise performing duties on behalf of Commission, or
(c) in the course of the provision (including the provision by another person) of a service to the Commission.

*3. Subhead**s** (1) **and (2)** 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 **strictly** 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 **reasonable** 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 **as is required by law or an enactment** .*

~~(e) disclosure of information to a public authority, whether in the State of otherwise, for the purpose of facilitating cooperation between the Commission and such authority in the performance of their respective functions.~~ ”~~16~~

We also note that the GDPR reference in the explanatory notes to Head 14 is incorrect and that it should refer to Article 54.2 of the GDPR.

3 (C) CHILD'S CONSENT IN RELATION TO INFORMATION SOCIETY SERVICES (HEAD 16)

Safeguarding privacy and consent are important to every business in building and maintaining the trust and safety of customers in the digital economy. The digital age of consent is a key issue for information society services and we note that the age of consent in relation to information society services is the subject of a separate consultation process.

[16] Deletion of subhead 3(e) is suggested on the basis that sharing of personal data by public bodies ought to expressly provided for by law or enactment (as per subhead 3(d)) rather than pursuant to a general reference to facilitating co-operation.

Separate submissions have been made on the appropriate digital age of consent and we look forward to notice of the Government's decision following the outcome of that consultation.

3 (D) WIDE SCOPE OF INVESTIGATIVE POWERS (HEADS 66 AND 67)

(D.1) Under the DP Bill the investigative powers of the DPC (or an "authorised officer") include the following:

> i. to investigate any infringement of DP law where it is " *of the opinion, for whatever reason* " that there may be an infringement (Head 66(1)(a));
> ii. to carry out a data protection audit as it " *considers appropriate* " to determine whether the " *practices and procedures* " of a controller/processor comply with DP law (Head 66(1)(b));
>
> iii. to enter the premises and take records or information of the data controller/processor without a search warrant (save where the premise is a private dwelling or where the authorised officer is impeded in gaining access) (Head 67); and
>
> iv. to require any person in a position to facilitate access to documents/records to provide " *all reasonable assistance* " to the authorised officer, including the giving of any *password necessary to make the documents concerned legible and comprehensible.* " (Head 67)

These powers are unquestionably wide and we have some concerns about the fact that they can, in the majority of circumstances, be exercised without a court issued warrant. Warrant-free powers are inappropriate for regulating data protection compliance particularly in circumstances where there is the potential for criminal prosecutions. For example under the existing Data Protection Act 1998 in England in order to enter premises a warrant is required and will only be issued if the court:

> *"is satisfied by information on oath supplied by the Commissioner that there are reasonable grounds for suspecting*
>
> *(a) that a data controller has contravened or is contravening any of the data protection principles, or*
>
> *(b) that an offence under this Act has been or is being committed,*
>
> *and that evidence of the contravention or of the commission of the offence is to be found on any premises specified in the information, he may, subject to sub-paragraph (2) and paragraph 2, grant a warrant to the Commissioner."*

We note that under the Competition and Consumer Protection Act 2014 that a warrant is required in connection with investigation of offences related to the Competition Act 2002 and suggest that a similar approach should be adopted in the DP Bill. We are also concerned about the low threshold for obtaining a search warrant (i.e. "reasonable grounds for *suspecting* that information required by an authorised officer for the purposes of exercising his or her powers is held at any premises or place…") particularly when compared to the current standard required in other Member States for search and entry.

(D.2) We also have concerns that the DP Bill does not provide clarity in relation to the circumstances in which a data protection audit may be commenced, for example, will reasonable notice be provided? Authorised officers' power to secure information,

documentation or premises for later inspection also carries a significant risk of blocking business while an audit is being performed, an audit which can occur even where there is no reasonable grounds to believe that an infringement of the GDPR has/is occurring. We submit that taking into account the broad powers of inspection which are provided for in this head provision for later inspection is excessive in the circumstances.

(D.3) We further note that an obligation to provide passwords necessary to make records legible and comprehensible is a feature of a limited number of regulatory regimes in Ireland (i.e. the Central Bank, Director of Corporate Enforcement and the Revenue Commissioners) but submits that such an obligation is not a requirement of the GDPR and is inappropriate given the number of other powers available to authorised officers and to the obligations of controllers and processors to assist authorised officers with their investigations.

(D.4) In addition, we note that a number of regulators in Ireland have produced public manuals or guidance as to how they operate their powers, with the Central Bank being one example and submits that public consultation on the shape of the DPC's policy surrounding the use of its powers is important.

3 (E) WRITTEN PROCEDURE (HEAD 73)

Power to require a report (Head 73)

Head 73 provides that the Commission may require a processor or controller to provide an independent report on any matter identified by the Commission.

In brief, this proposal involves the following:

> i. The DPC can direct that a controller or processor provide the DPC with a report on a specified matter prepared by an independent reviewer.
> ii. The controller/processor must nominate to the DPC a suitably expert and independent person to carry out the reviewer function. The DPC can accept that nomination or appoint a different person in his/her place.
> iii. A contract must be entered into with the reviewer and the controller/processor is responsible for paying the reviewer's fees.
> iv. The controller/processor is required to co-operate with the reviewer and provide information/documentation requested.
> v. The controller prepares a report and delivers it to the DPC. The report does not bind the DPC but may be relied upon by the DPC.

Ibec has grave concerns about this provision. The DP Bill cites Article 58(4) of the GDPR as allowing for additional powers but the GDPR does not mandate or even refer to inclusion of an expert report procedure. Indeed Ibec questions the justification for such a procedure given the extensive references throughout the GDPR to the accountability principle and the onerous obligations on data controllers and processors to be responsible for, and be able to demonstrate compliance, with the obligations contained therein.

The procedure is an entirely new investigative tool that is based on a procedure used by the Irish Central Bank to investigate breaches of financial regulation by banks. We submit that absent a proper explanation as to why this invasive and expensive procedure is required (for example, are the powers of authorised officers not sufficient to conduct investigations?), it ought to be removed from the DP Bill.

The Commission may already investigate, audit and request information – it is not appropriate to require the entity under investigation to prepare an investigation report on

itself. If the report provision is to be retained in the Bill, it should be subject to reasonable safeguards and requirements, such as a reasonable opinion of a contravention of the Bill or GDPR.

Paragraph 10 provides that the costs of and incidental to the preparation of a report prepared under this head shall be borne by the controller or processor. Paragraphs 7 and 9 further provide that while it is the controller or processor who will enter into the contract with the reviewer, this contract may be reviewed and modified by the Commission. Further again, paragraphs 13 and 14 make it clear that the Commission will not be bound by the content of the report or by any course of action recommended by the report. Effectively, the full costs of the report will, therefore, be borne by the controller or processor notwithstanding the facts that (a) the Commission may determine the level of the costs both by way of its veto power and its power to require specific and additional tasks of the reviewer and (b) despite the incurring of potentially substantial costs in preparing the report, it may be subsequently ignored by the Commission.

Ibec is concerned that this provision places a disproportionate additional burden on businesses and employers and effectively enables the Commission to contract out and pass on the cost of monitoring compliance with the GDPR and the Act to businesses and employers. Furthermore, it introduces an unknown cost for any organisation preparing for GDPR and fails to take account of organisational budgeting processes. While Ibec notes the reference to the Commission taking into account “the level of resources available to the controller”, there does not appear to be any obligation on the Commission to take into account reasonable representation from the controller or processor. Ibec, therefore, does not believe this will provide sufficient comfort to employers. In Ibec’s view, the Commission should be provided with a sufficient budget for the completion of its tasks rather than passing on this cost and obligation to the private sector.

The provision at paragraph 16 for criminal liability to attach to certain actions in relation to the preparation of the report is particularly concerning. This is all the more so given that despite the severity of the sanction proposed the language contained in the provision is very vague. For example, paragraph 16 provides that a person who “obstructs or impedes a reviewer in the preparation of a report” will be guilty of a criminal offence punishable by summary conviction or conviction on indictment. However, the exact meaning of “obstruct or impede” is not at all clear. Could it include a business attempting to negotiate a fairer price for the provision of the review and thereby refusing to sign a contract until such a price is agreed?

Finally, the situations in which this procedure may be used have been defined in overly broad terms - at the most it should be limited to situations where specialist knowledge, not in the possession of the DPC, is needed to conduct an investigation.

3(F) APPLICATION TO PUBLIC AUTHORITIES

Ibec is concerned that the general scheme fails to provide a definition for “public authority”. In the absence of a definition for “public authority” in the GDPR, it is important that the DP Bill provides certainty in this regard.

Furthermore, Ibec has some reservations about the proposal to only impose administrative fines on public authorities insofar as they are acting as undertakings. Whether a body is acting for gain or not, it seems more equitable to apply the same rules to the private and public sector.

4. Education and awareness on data and data protection is important in growing our digital economy

As stated in Section 1, the use of digital tools and data can be leveraged to create growth and jobs across the broader economy. Data protection is not only about protecting rights but about safeguarding our growing digital economy. We need to build a greater understanding of this value across the economy and society.

4 (A) BUSINESS INITITATIVES

Ibec and its members are playing their part and have established groups that look at data policy and raising awareness and understanding of the upcoming GDPR, specifically Ibec has:

- Developed a series of free guidance documents aimed at helping businesses in their preparations for compliance with the GDPR.
- Staged a well attended series of free regional events, 'delivering the digital age', which dealt with digital innovation and data protection – representatives from the Office of the Data Protection Commissioner addressed each of the events. The events were held in Dublin, Limerick, Athlone, Galway, Cork, Kilkenny and Sligo between April 26 and May 25.
- Sponsored and participated in the Government's recent Data Summit on June 15-16.

4 (B) FREEDOM OF EXPRESSION

Head 24 of the DP Bill purports to give effect to Article 85 of the GDPR. Head 24 provides that personal data processed "for *journalistic purposes and for the purposes of academic, artistic or literary expression* "shall be exempt from certain provisions of the GDPR having regard to the right to freedom of expression and information.

Article 85 of the GDPR imposes an obligation on Member States to reconcile the rights conferred by the GDPR with the right to freedom of expression and information "including *processing for journalistic purposes and the purposes of academic, artistic or literary expression."*

Head 24 has been drafted such that the exemptions within the Bill only apply to the examples included within the GDPR (i.e. journalistic purposes or academic, artistic or literary expressions). It is clear from the text of Article 84 that these identified purposes are not supposed to be a closed list and that Head 24 does not therefore give full effect to Article 85. We would be strongly in favour of including within Head 24 the broad right to freedom of expression and information to reflect Article 85. In order to address this concern we suggest that the following text is added to Head 24(1):

> *"Personal data processed* ***for the purposes of the right to freedom of expression and information, including*** *processing 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."*

The Bill would also benefit from a more effective articulation of the balancing to be done between (i) freedom of expression and information and (ii) data protection.

The case-stated procedure in subhead 3 has the potential to cause additional complexity. Further consideration should be given to the interaction between the case-stated procedure and the complaints and adjudicative processes, including instances when the consistency mechanism under the 'one stop shop' is triggered.

5. Resourcing our data protection and cybersecurity capacities is important to growing our digital economy

The entry into force of the EU General Data Protection Regulation (GDPR) and this Bill, when drafted and enacted, in May 2018, will have significant implications for the workload of the Office of the Data Protection Commissioner. The workload is likely to increase, and investigations will become more complex, especially those with cross-border aspects. Ibec called for extra investment in our national data protection and cybersecurity capacities in Budget 2017[17] and welcomed the news that the resources of the Office of the Data Protection Commissioner have been increased to €7.526 million for 2017, up from €1.9 million in 2014.

The issue of any further resource requirements will be considered in the context of the Estimates for 2018. Ibec believes that policy makers must continue to ensure that the Office of the Data Protection Commissioner continues have the resources adequate to its role as a key regulator in Europe's data protection framework.

Ibec also submits that new courses of study for privacy engineering would be useful. With the coming into force of the GDPR and this DP Bill, new types of professional positions, including data protection officers and privacy operations teams, will be created in the data protection / privacy profession. Individuals occupying these roles will have to determine, amongst other matters, how to implement accountability obligations and privacy by design. These roles will be more fundamentally "hands-on" and wrapped up in the technical details of managing consent, notice, design and oversight, and will be required in addition to the legal resources required to ensure compliance in an organisation.

6. Specific comments on the general scheme of the Data Protection Bill 2017

Processing of personal data in the context of the employment relationship (Heads 18 and 19)

Ibec welcomes the confirmation in Head 18 (albeit also provided for in the GDPR itself) that special categories of personal data may be processed where necessary for the assessment of the working capacity of the employee and for carrying out obligations and exercising specific rights of the controller or data subject in the field of employment law. We also acknowledge the provision at Head 19 which permits controllers and processors to process personal data relating to criminal convictions and offences where such processing is necessary to protect the public against harm arising from dishonesty or the unfitness or incompetence of persons authorised to carry on a profession or other activity.

Ibec would, however, like to see further clarity on the extent and scope of these draft provisions. For example, there is significant uncertainty surrounding the phrase "subject to

[17] See www.ibec.ie/digitaleconomy

suitable and specific measures to safeguard the rights and interests of the data subject" in Head 18 and "subject to appropriate safeguards" in Head 19. Ibec would therefore welcome further clarity on this point but would caution against adding to the already onerous administrative and record keeping obligations of employers both in the fields of employment law and data protection law. The explanatory note at Head 18 states that the 'possibility of including a toolbox of possible safeguards in a new subhead will be explored during drafting'. If this possibility is pursued then industry and other stakeholders should be engaged on best practice.

In light of the continuing uncertainty as to the extent to which safeguards are intended to be additional or complementary to data controller obligations already required under Articles 24 (*Obligation to have Appropriate Technical & Organisational measures and Demonstrate Compliance*), 25 (*Privacy by Design*) and 32 (*Security*), we wish to highlight the importance of public consultation on the contents of the "toolbox".

We note that Article 89 of the GDPR also permits derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes where appropriate safeguards are in place and Head 25(4) provides for "appropriate safeguards" to be put in place in connection with such processing. We suggest that the public consultation on the toolbox in the context of processing special categories of data and data relating to criminal convictions ought to extend to the safeguards referenced in Head 25(4).

In contrast to the lack of detail referred to above, Ibec believes that Head 18(5) is too narrow. It seems to Ibec that there may be other legitimate reasons to process biometric data, with full consent, other than identification and security. Rather than constrain innovation, therefore, Ibec suggests that this detail be omitted.

Processing of personal data (Head 19)

In accordance with Article 10 GDPR, Head 19 helpfully specifies circumstances in which processing of personal data relating to criminal convictions and offences may be processed. It is important that the DP Bill also explicitly provides that that processing of personal data relating to criminal convictions and offences which is necessary to comply with applicable legislation is permitted. By omitting this explicit reference, uncertainty is created as to whether any current processing of such personal data which would not fit within the specific purposes specified in the DP Bill but done under other applicable laws would be compliant with the DP Bill. For example Head 19(1)(b) could be amended in the following manner:

"(b) processing is necessary for purposes of exercising a regulatory, authorising or licensing function or determining eligibility for benefits or services ***, or required by or permitted under applicable legislation.*** *"*

Some organisations are required to comply with anti-money laundering requirements, sanctions and fitness and probity requirements. It is implicit in complying within many of these requirements that certain organisations have to process personal data which relates to criminal convictions or the suspicion of criminal activities. Profiling activities for the purposes of the GDPR may also be required for these purposes.

It is not clear why Head 19 *"Processing of personal data relating to criminal convictions and offences (Article 10)"* does not make provision for derogations covering these issues. It would helpful if similar provision could be made under Head 19 as is currently provided for under Head 20. Conversely, the fraud management provision in Head 19 could perhaps also

be included under Head 20. It is not clear why this would be under one heading but not another.

Restrictions on exercise of data subject rights (Head 20)

Ibec notes that the general scheme provides for further regulations to be made in respect of the restriction of the rights and obligations provided for in Articles 12 to 22 and Article 34 of the GDPR. Ibec will be happy to engage with the relevant Ministers in respect of the making of such regulations.

Article 23(1)(i) of the GDPR allows for limitation to the right of access to safeguard the protection of the data subject or the rights and freedoms of others. Article 15(4) also provides that the right of access shall not adversely affect the rights and freedoms of others. Rights and freedoms of others include the rights and freedoms of the data subjects as well as those of the controllers (e.g. the right to conduct a business). The DP Bill should therefore provide for the following limitations to the right of access:

- Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, the controller should not be obliged to comply with the request unless the other individual has consented to the disclosure of the information to the person making the request.
- Intellectual property rights should be protected and controllers should not be required to provide access to data subjects if doing so would require giving access to information protected by intellectual property law.
- Where the provision of such information proves impossible or would involve a disproportionate effort from the controller. There are some data elements that are stored in such a way that requiring controllers to provide them to data subjects would entail an enormous financial and resource burden that would not be commensurate with the value of the data to the data subject.

Ibec notes that this head allows for restrictions on a data subject's right to access their data, in the interest of, *inter alia*, "preventing, detecting, investigating or prosecuting criminal or disciplinary offences and the execution of penalties".

A situation which may require legislative attention arises where a data subject contacts a relevant operator seeking a copy of any requests made by An Garda Síochána or any other state agency to access his personal data for the purposes of a criminal investigation.

In such cases it can be administratively difficult and potentially inappropriate for the relevant operator to ascertain from the relevant authority or investigating officer whether the disclosure of such information to the data subject is likely to impede an ongoing investigation.

We note that EU law (for example, see CJEU case C-203/15 Tele2 Sverige and C-698/15 Watson) requires that relevant State agencies to whom access to the retained data has been granted should notify the persons affected, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those agencies.

Ibec believes that this is a sensible approach, having regard to the objective of effective investigation and prosecution of offences, and would welcome legislative guidance on this point.

Data protection by design and by default (Head 41)

Perhaps outside the scope of this review but relevant nonetheless is what influence and incentives the State will provide towards implementing the necessary regimes for Privacy by Design and Privacy by Default referred to in this Head. These regimes are determining factors as to why education needs to evolve to create the talent pool necessary to deliver on what essentially will be a new profession, that of Privacy Engineering. An example of how academia is addressing this in the U.S.is from Carnegie Mellon: http://privacy.cs.cmu.edu/.

Data logging obligations (Head 44)

It seems ambiguous, as stated in subhead 6, as to what is the procedure to extend the timeline from May 2023 to May 2026. For example, does this require an exemption to be granted by the ODPC? This is a relevant point as the period May 2018 will shift the focus from the *paper compliance* activities that will dominate the GDPR implementation activities to the *effective compliance* actions that will take place after. For many organizations the timeline to migrate legacy systems to be compliant by May 2026 instead of the more onerous May 2023 deadline will be necessary and availed of.

Procedural safeguards (Part 5)

Ibec welcomes the acknowledgement in the general scheme that the possibility of stringent sanctions arising from the investigation of complaints or the conduct of data protection audits means that rigorous procedural safeguards and due process must be maintained. However, Ibec believes that the general scheme, as currently drafted, does not so ensure such procedural fairness.

Chapter 3 sets out some detail as to the conduct of investigations by the Commission. In particular, Head 74 paragraph 4 provides that an authorised officer charged with an investigation may afford a controller or processor an opportunity to respond to an allegation within 21 days, or such further period not exceeding 21 days. Equally, Head 76 provides that a controller or processor must make any submissions on the content of a draft investigation report within 21 days, or such further period not exceeding 21 days. These time limits are far too short and fail to allow for the increasingly complex nature of many data protection complaints and the need to allow sufficient time to organisations to properly respond to complaints or other investigations. Furthermore, Ibec does not believe that the decision to extend the timeline should be solely at the discretion of the authorised officer in the absence of any oversight or right of appeal. Ibec is, therefore, disappointed that despite the acknowledgment of the need to ensure due process and rigorous procedural safeguards, the time limits provided for in the general scheme risk organisations not being afforded sufficient time to properly represent themselves.

Ibec is similarly concerned by the time limits of 30 days to appeal a decision of the Commission to impose a fine, and 28 days to appeal other legally binding decisions of the Commission as set out in Heads 69, 70, 71 and 79.

Head 80 paragraph 2 provides that in circumstances where an organisation does not appeal the imposition of a fine, the Circuit Court shall confirm the fine “unless the Court sees good reason not to do so”. Ibec would welcome further clarity on what this might mean.

We note that in the course of the pre-legislative scrutiny it was suggested that the GDPR may allow for class actions. The relevant provision of the GDPR (Article 80) only permits a third party to take an action on behalf of a data subject where such actions are provided for by way of national law. Class actions are not possible today in the State and we submit that

the provision for class actions would be a significant development for Irish law. Any such proposed development and would require detailed consultation if consideration is being given to its introduction as part of the DP Bill or otherwise.

Clarification is required on whether the state intends to implement the identification service necessary under the GDPR to, for example, differentiate between adults & children. If the onus falls to the market, and not the state, then this should be clarified sooner rather than later to allow solutions to be readied in time by businesses for GDPR enactment in May 2018.