DÁIL ÉIREANN

AN COMHCHOISTE UM DHLÍ AGUS CEART AGUS COMHIONANNAS

JOINT COMMITTEE ON JUSTICE AND EQUALITY

Dé Céadaoin, 14 Meitheamh 2017

Wednesday, 14 June 2017

Tháinig an Comhchoiste le chéile ag 9 a.m.

The Joint Committee met at 9 a.m.

Comhaltaí a bhí i láthair/Members present:

Teachtaí Dála/Deputies	Seanadóirí/Senators
Colm Brophy,	Frances Black,
Jack Chambers,	Martin Conway,
Clare Daly,	Niall Ó Donnghaile.
Jim O'Callaghan,	
Mick Wallace.	

I láthair/In attendance: Deputy Pat Buckley.

Teachta/Deputy Caoimhghín Ó Caoláin sa Chathaoir/in the Chair.

General Scheme of Data Protection Bill 2017: Discussion

Chairman: I have received no apologies. I thank the members and attendees for being here and on time. The item for discussion is the general scheme of the Data Protection Bill 2017. Our first engagement is with Department officials. I welcome Mr. Seamus Carroll, Ms Noreen Walsh and Mr. Conor O'Riordan from the Department of Justice and Equality. I acknowledge the presence in the Gallery of the Data Protection Commissioner, Ms Helen Dixon, and welcome her. I understand she is joined by Mr. John O'Dwyer, Ms Anna Morgan and Ms Emily Burke. I hope I have identified everyone properly. On behalf of the committee, I thank all of the witnesses for their attendance today to discuss this important Bill. The format of the meeting is that the witnesses will be invited to make an opening statement and this will be followed by a question and answer session.

Before we begin, I draw to the attention of witnesses to the situation in regard to privilege. Please note that they are protected by absolute privilege in respect of the evidence they are to give to the committee. However, if they are directed by the committee to cease giving evidence on a particular matter and they continue to so do, they are entitled thereafter only to a qualified privilege in respect of their evidence. They are directed that only evidence connected with the subject matter of these proceedings is to be given and they are asked to respect the parliamentary practice to the effect that, where possible, they should not criticise or make charges against any person, persons or entity by name or in such a way as to make him, her or it identifiable.

I once again remind members that, under the salient rulings of the Chair, they should not comment on, criticise or make charges against a person outside the House or an official either by name or in such a way as to make him or her identifiable.

I invite Mr. Seamus Carroll to make his opening statement.

Mr. Seamus Carroll: I thank the Chairman 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, Ms Noreen Walsh and Mr. 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 Justice and Home Affairs, 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 were published in May 2016. The first was a regulation containing general data protection rules while the second was 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. 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 decided to propose both a regulation and a directive and it 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. First, there is the introduction of a new legal basis for data protection standards in Article 16 of the Treaty on the Functioning of the European Union, TFEU, together

with the introduction of the right to data protection in Article 8 of the EU Charter of Fundamental Rights. Second, there is 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. Third, there is the rapidly developing case law of the Court of Justice in relation to the protection of personal data. Finally, there is 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 - referred to as 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, known as data controllers and data processors.

More concretely, both instruments place increased emphasis on the following. First is 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. Second, there is also an emphasis on 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 written arrangements with any data processors acting on their behalf. Third, there is an emphasis on security. Personal data must be processed in a manner that ensures appropriate security standards, that is to say, 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 which sets out data subject rights and 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. First, it aims to give further effect in national law to the regulation where permitted by the regulation. Second, it aims to transpose the directive into national law. Third, it aims 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 contains a number of standard provisions. With regard to 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.

On 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 Commis-

sioner. 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, including investigative powers, corrective powers, authorisation and advisory powers, on the 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 €7.526 million for 2017, up from €1.9 million 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 by the end of this year. The issue of any further resource requirements for 2018 will be considered in the context of the Estimates 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, that is the data protection authority of the member state in which an entity's main establishment, or indeed 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 inquiry 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 for further consideration. The board, which will comprise representatives of all supervisory authorities across the EU, 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.

The data protection regulation is somewhat unusual in so far as it provides a certain margin of flexibility for member states, especially in respect of data processing activities undertaken by their public sectors. That gives rise to the need for implementing national law. Part 3

seeks, therefore, to give further effect in national law to various articles of the regulation that allow a margin of flexibility. Head 16, which is blank for the present while awaiting a specific Government decision on the matter, 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 purpose. 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 Commissioner 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 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 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 any other entity authorised by national law to exercise public authority and public powers for the same purposes.

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 and so forth

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 instead 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 organisational 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 contains 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 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, for example, the information and enforcement notices, while others are new, for example, the power to seek a High Court order to suspend or restrict data processing or data transfers to a third country or the 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. A number of safeguards, therefore, have been included in this part. First, the investigative functions under heads 74 to 76 and the adjudicative functions under heads 77 and 78 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. Second, provision is being made not only for appeals against administrative fines, under head 79, but for confirmation of fines by the Circuit Court in the event that they have not been appealed, as per head 80. In the latter case, the role of the court will be to confirm that due process has been observed.

Moving on to 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 Departments, public authorities, representative bodies and the Data Protection Commissioner during preparation of the general scheme of the Bill. However, 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.

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 European Court of Justice will help to ensure that data protection will remain an active and challenging area of law in the years ahead. I hope that I have provided the committee with some clarity on the content of the Bill and the background to it. We are happy to respond to any questions that members may have and I thank them for their attention.

Chairman: Thank you very much Mr. Carroll. I now invite members of the committee to contribute. Deputy Daly is first.

Deputy Clare Daly: Unfortunately, I have to leave at 9.50 a.m. so I apologise to the Data Protection Commissioner as I will not be able to stay for that presentation. This is the first day of what will be a sizeable body of work for the committee. It is incredibly technical work in some ways, and a bit of snoozefest in some ways as a result, although I am not talking about the presentations, of course. Separate to that, however, the issues of privacy and transparency are obviously critical and the question of how we balance that, bring it out and engage with stakeholders will be important.

While I am not hugely prepared on the issue, I will work on the basis of a Ladybird version, given the points made by Mr. Carroll about the backdrop to this being higher EU data protection standards and also the rapidly developing case law from the EU Court of Justice. We have had the implications of the Barrett judgment in regard to information in the context of the recent actions on the public services card and the individual health identifier. In that scenario, we have one arm of Government, if one likes, engaged in a course of action of sharing data which seems to be blatantly against what the Barrett judgment states about Departments not being allowed to share information without prior consent. Given that is happening now, how will this Bill impact going forward? Mr. Carroll said this will be brought forward in the autumn. Will this project have to be abandoned in the autumn as a result or do we have any indication of the implications at this stage?

Mr. Seamus Carroll: I thank the Deputy for the question. The Barrett judgment is, of course, very interesting. It dates from October 2015 and highlights two requirements. First, there must be an adequate legal basis for the sharing of personal data between bodies. Second, and this is a crucial point in the judgment, it is not sufficient that there be a legal basis; there

must also be full transparency where public bodies are sharing data with each other. For example, that could involve providing adequate information on the websites of the bodies concerned as to the sharing arrangements which are in place.

Consent is not always a requirement when it comes to dealing with public bodies. For example, when it comes to taxation matters, consent has little role to play and what the Revenue Commissioners do is underpinned by legislation, not by consent. Whereas consent may provide a valid legal basis for the processing in many cases, when it comes to the activities of public authorities and bodies, a statutory basis is necessary - a basis in law rather than a basis in consent or in contract.

I do not particularly want to be drawn into the detail of the health legislation, which is being considered separately. However, going back to the point the Deputy raised for the future, there must be a lawful basis for the processing and there must also be greatly increased transparency. As I said earlier, whether it is a public or a private body, and we often see terms and conditions on websites that would require considerable effort to understand, for the future this must be much more transparent and must be written in clear and plain language that can be readily understood.

Deputy Clare Daly: I am not sure I am very clear as a result of that reply. People would obviously understand the issue of consent in regard to Revenue matters because the public understands there is an overriding public interest as to why people should pay their taxes. The sharing of information in that regard is broadly understood. However, the health database does not have a legislative base. Mr. Carroll mentioned health legislation being developed separately. The database is actually under construction and the sharing of information is already under way, but most people not only do not understand why there is a public interest, but do not even know that their information is being shared in this way. Basically, every single aspect of a person's identity from a health point of view is being put together in one database, where their identity is being signed off. I am not sure that would meet the bar on transparency that is required in this instance. In that sense, I wonder, given that we are on the cusp of such an important project, why a body of work which could contradict that is going on simultaneously. Maybe it is outside the scope of the Department of Justice and Equality because other Departments are running it.

Mr. Carroll said that head 40 states that the competent authorities must adopt and implement appropriate technical and organisational measures to ensure they demonstrate compliance with the standards. It has obviously been a matter of considerable public debate, given the issues about gardaí accessing PULSE records to check up on ex-girlfriends, the cases of giving information to the Department of Social Protection and all the rest, and even my own case with the Garda. In light of such issues, head 23 makes provision for administrative fines in a limited way but it does not really deal with those situations because the bodies will only be subject to them if they are providing goods and services in the same market as private companies. Do we need to beef that up? There does not seem to be any real sanction in the Bill other than a limited one of administrative fines for public bodies, which is not much of a deterrent in terms of breaches.

Mr. Seamus Carroll: To go back to the first question, there is a very important safeguard in this legislation, which is that data controllers must carry out a data protection impact assessment where there is likely to be risk to the rights and freedoms of individuals. In certain cases, in the preparation of legislation in particular, public bodies and authorities must consult with the Data Protection Commissioner. In regard to the health matters mentioned by the Deputy, I understand, and perhaps the commissioner can confirm this, that consultations have already

taken place with the health committee on this matter.

The corrective powers of the commission with regard to the private sector are set out in the regulation but very important corrective powers in regard to public authorities and bodies are also set out in head 61, including those bodies mentioned by the Deputy. The corrective powers are set out in paragraph (2) and include the issuing of warnings to a competent authority to issue reprimands, ordering a competent authority to comply with a data subject request, ordering a competent authority to bring processing into compliance with this part of the Act, ordering a competent authority to communicate a breach to the data subjects, imposing a restriction on processing, and ordering the suspension of data transfers to a recipient in a third country. There is quite a broad range of corrective powers which the commission will have in respect of public authorities and bodies within this Act. That is quite separate from the corrective powers which are conferred directly on the commissioner under the regulation.

Deputy Clare Daly: Thank you.

Deputy Jim O'Callaghan: I thank Mr. Carroll for his presentation. The EU seems to be doing its best to make the regulation of data protection as impenetrable as possible, as we see from the regulations and directives. To make a general point, we have laws in this country dealing with data protection and when this Bill is enacted, the laws will be extended. Will it be the case that there will be a group of people who will then be covered by data protection law who at present are not covered, or is it that individuals will remain the same and that there will be a greater emphasis on certain areas?

Mr. Seamus Carroll: Our current data protection law - the 1998 and 2003 Acts - covers all data processing operations. The rights are conferred on data subjects and the obligations are imposed on data controllers and data processors. I accept the Deputy's point about it being impenetrable because we are even using a different language of "data subject" instead of "individual" and "data controller" instead of "public body", so it has a vocabulary of its own which does not make it any easier to understand. What the regulation does and what this legislation will do in transposing the directive is raise the standards of data protection to increase the rights of individuals and extend the obligations on those who process personal data. The regulation and the directive provide for a more detailed application of rules with a view to achieving greater harmonisation across the European Union. The current data protection directive dating from 1995 has 30 articles. The GDPR has 90, while the new directive has 60. That is a rough indication of the increased complexity.

When it comes to scope, individuals will be exempt to the extent that the so-called household exemption will apply. Where individuals are processing data for personal or household purposes, data protection law does not apply. Other than that, the scope will be similar to that of the current-----

Deputy Jim O'Callaghan: On the age of consent for children, does it mean that data processors cannot use information accessed by them in the case of children under the age of consent?

Mr. Seamus Carroll: Article 8 is about the offering of information society services to individuals up to the age of 17 years. When the draft regulation left the JHA Council, the age threshold was under 13 years in order that in the case of children up to the age of 12, parental consent would be required or at least the person offering the information society services would have to make the best effort to obtain parental consent for them. When it went to the European

Parliament, the age threshold was increased to 17 years. That means that under the law those aged up to 16 years require parental consent, but there is a provision for member states to reduce it to 13.

Deputy Jim O'Callaghan: It is a policy decision for the Government what the age should be. Let us assume a child is aged 12 years as he or she will be covered, no matter which age threshold is applied. Can the child's parents make a complaint to the Data Protection Commissioner if it appears to be the case that the child has been offered something on social media for which consent has not been provided?

Mr. Seamus Carroll: The difficulty is that the services are being offered online. The obligation under Article 8 of the regulation is that the controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility taking into consideration the available technology. The threshold is that the offerer of the information society services must make reasonable efforts. There is similar legislation in place in the United States - the Children's Online Privacy Protection Act 1998. The European provision draws inspiration from the American legislation, but it is a threshold of "reasonable efforts" because, clearly, at such a distance, it is difficult for the offerer of the information society services to be certain about the age of the child.

Deputy Jim O'Callaghan: One of the reasons I have asked about this is that Mr. Carroll correctly mentioned that the Office of the Data Protection Commissioner which will become known as the Data Protection Commission will expand considerably on the basis of the Bill. Currently, it has a staff of 100. Does Mr. Carroll agree that the new commission will become a large statutory body which will need to be significantly funded, particularly in the light of the fact that there will be complaints from other countries?

Mr. Seamus Carroll: Part 2 of the Bill which establishes the commission is predicated on an increase in workload. The office is being geared up for an increased workload because the staff number is approaching 100. As to what future demand will be, I am sure the commissioner will be able to give some idea of current thinking but, at least for the moment, the office is being geared up to address the expected increase with the necessary expertise. That is also the reason the possibility of increasing the number of commissioners is being provided for. There will undoubtedly be an increase in workload and the complexity of the cases being dealt with by the commission.

Deputy Jim O'Callaghan: People have an entitlement to seek compensation. They can go to the courts if their data have been breached or they can go down the statutory route under the legislation. If compensation is awarded, will the new commission order the breacher to pay it?

Mr. Seamus Carroll: The position is that compensation may only be obtained from a court. The Data Protection Commissioner is not in a position to award compensation. That will be a matter for a court and it is covered in Part 6. It is important, however, that the liability of those handling personal data be extended to non-material damage. This is significant because current case law in this jurisdiction means that compensation is only payable for material loss, but the new rules will also extend this to non-material damage such as distress or humiliation.

Deputy Jim O'Callaghan: Am I correct that under head 58, therefore, only a court can award compensation?

Mr. Seamus Carroll: Yes. Head 91 makes provision for claiming compensation through

a court.

Deputy Jim O'Callaghan: Many large corporations have access to huge volumes of data for individuals. Are there proposals to impose responsibility or liability on such holders of data? I acknowledge that Mr. Carroll is not in the business of engaging in a discussion of policy, but does the regulation or the directive take into account responsibilities that rest elsewhere and the necessity to fund them?

Mr. Seamus Carroll: Data protection principles require that data be used for the purposes for which they are collected and not for another purpose incompatible with them. There is an enhanced right in Article 17 of the regulation to seek erasure of personal data. In the part which gives effect to the directive it is made clear that data controllers or, in other words, competent authorities must also ensure they have retention periods for personal data or that they have policies governing the retention periods. As the Deputy said, there is increased emphasis on the right to seek erasure of personal data. There is also an enhanced accountability principle, whereby data controllers and processors, be they in the private or the public sector, must demonstrate compliance with these instruments and the Data Protection Commission will have a clear power to carry out audits. It will, therefore, not necessarily wait for complaints to arrive to carry out its enforcement activity. It may take a more active role with this audit facility.

Deputy Jack Chambers: I thank Mr. Carroll for a comprehensive presentation. I refer to the right to be forgotten under Article 17. Where a child does not have the capacity at the time to consent, how will it work in the context of the Bill? How will it be implemented in practice in the interaction with organisations? Will regulations issue to make it workable in the context of the Bill?

Mr. Seamus Carroll: There is the right under current law to seek erasure, but that right is being beefed up in the regulation. It will be a matter for individuals to exercise their right against the data controller. In the event that the right to seek erasure is refused, a complaint will be brought to the Data Protection Commission which will will investigate. One of its powers will be to order the controller to comply with a request from a data subject. In the event of that not happening, various corrective powers are provided, including, for example, the imposition of an administration fine.

Deputy Jack Chambers: On a separate point - Deputy O'Callaghan referred to the issue of compensation - does Mr. Carroll fear that this Bill, without providing for an explicit mechanism for people to have a positive ability to receive compensation, will inevitably end up clogging up the courts with potential breaches of data control, whereby large organisations and corporate bodies would have the ability to take on individuals? Would it not be better to provide stronger legislation that would provide for a positive right to compensation so that we better achieve this balance?

Mr. Seamus Carroll: The Deputy is right to draw attention to compensation as being one of the key issues for the future. As we mentioned earlier, there are enhanced data subject rights and the strengthened obligations on controllers, and if the data controllers are not in a position to demonstrate compliance, there is a twofold risk. The first is the risk of compensation claims. As I have mentioned already, the liability is being extended to non-material damage. For instance, if a public body simply ignores requests it receives, this may result in distress for an individual which might then form the basis of a compensation claim. Second, there is the added possibility of administrative fines, particularly in the case of private sector bodies, so it is very much in the interest of data controllers and processors to ensure they comply with the law so

as not to incur the risk of compensation claims and administrative fines. There is undoubtedly the risk that there will be an increase in compensation claims. This will depend on the extent to which controllers and processors comply with the new data protection standards. If they do not comply, there is every risk that claims will be brought within the courts. Case law will develop over time, but the Deputy is right to draw attention to this as one of the serious implications of this legislation.

Deputy Jack Chambers: I have a final question. Regarding the derogation in head 24, how will this balance be achieved in the context of, for example, social media organisations allowing freedom of expression on the one hand and data control on the other? Could head 24 allow corporations or other data controllers potentially to derogate their responsibilities under the Act? How does Mr. Carroll see this working out in practice?

Mr. Seamus Carroll: The regulation itself makes clear that data protection is not an absolute right and that it must be balanced with other rights. Another fundamental right is the right to freedom of expression and information. Here there is the potential for a conflict arising between the right to data protection on the one hand and the right to freedom of expression on the other. It is likely in the future that this will be a source of litigation. The balancing of these rights is typically the kind of conflict that is resolved in the courts. It is for this reason that we have provided in subhead 3 that the Data Protection Commission may, upon its own initiative, refer any question of law arising in a case to the High Court for determination. The Data Protection Commission is not required to do this; this is a discretionary power it will have. We are therefore creating a case stated option here for the Data Protection Commission so that the matter of reconciling such fundamental rights, which is typically a matter for the courts, can also in this case be undertaken by the courts.

Deputy Jack Chambers: I wish to make a final point, to which Mr. Carroll does not have to respond. I thank all the witnesses for their work on this issue. One thing I fear from our interaction and from the beefed-up cost - €5 million in the past two years - is a potential for massive levels of case law and litigation. We must be wary of this and make this legislation work so that it does not become an enormously bureaucratic and costly process. We must protect the fundamental rights of individuals, but we must also be very careful not to create a monster that would make it very difficult for individuals to have their rights upheld. I fear we could be doing this even with the beefed-up cost of the Data Protection Commission and the potential for massive litigation as incorporated in the Bill. We just need to be aware of this. Perhaps there is legislation we can amend to ensure that this does not happen or perhaps we can provide compensation before the courts intervene. We must be watchful.

Chairman: Does Mr. Carroll wish to make a brief comment in response?

Mr. Seamus Carroll: I will make a very brief comment. Perhaps the Data Protection Commissioner will comment on this afterwards. It is very important for data controllers to gear up now. I am sure that litigation cannot be entirely avoided in the future because this is inevitably the result of creating higher standards and new rights. However, the more an awareness is created and adjustments are made in advance of this legislation, the smaller the risk of costly and lengthy litigation.

Chairman: Deputy Mick Wallace is indicating, and after his contribution I will call Senator Niall Ó Donnghaile. We have the second session to proceed with and a very busy schedule this morning, so I want to try to keep proceedings as tight as possible. If anyone else wishes to indicate in this session or if they wish to hold back for the Data Protection Commissioner, that

is fine. I call Deputy Wallace.

Deputy Mick Wallace: I thank Mr. Carroll for his presentation. I promise I will not talk for too long. I do not understand this matter as much as I would like to yet, but we will get there eventually. It is very complex and I can see problems on both sides. It will be very hard to get the legislation perfect in any form.

In April of this year, the Germans approved a bill giving effect to the General Data Protection Regulation, GDPR, which includes a specific provision on Article 82 of the GDPR. With regard to the general scheme of the Irish Bill, while there is a reference in the explanatory notes of head 24 to the fact that Article 82 of the GDPR provides that a person suffering material or non-material damage as a result of the infringement of the GDPR has a right to receive compensation, the general scheme of the Bill does not include an explicit right in this regard. The question here is whether the wording of Article 82 of the GDPR is clear enough to be horizontally effective or whether the right to compensation needs implementing legislation in Ireland which would give direct effect to Article 82 of the GDPR. If this matter is not cleared up in legislation, we could be leading ourselves open to compensation cases from Europe and elsewhere. Has the Department obtained legal advice as to whether Article 82 of the GDPR, concerning the right to receive compensation, needs national implementing legislation?

Mr. Seamus Carroll: That is a very interesting and important point. We are aware of the provision in German law. 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.

Deputy Mick Wallace: To follow up on Deputy Clare Daly's point about the Health Identifiers Act 2014, there is a plan to introduce an identity card. It is said it will not be compulsory. However, one will not be able to get a passport or driving licence without it, so the reality is that it will be compulsory. With the potential of cyberattacks and God knows what else now, and given that so much data seems to get leaked and invaded in one form or another, is it not worrying that information will be going on an identity card and that this may get into the hands of others? For example, if the identity card is introduced full-scale, will we be entitled to know what is put on it? I would also ask the same about passports. I saw my passport being put into a machine at a passport point recently, and the person operating the machine seemed to find what he was reading incredibly interesting. I would love to know myself what is on it. Are we entitled to know what is put on these things or not?

Mr. Seamus Carroll: I think the Deputy is trying to tempt me out of my comfort zone on this and I will resist the temptation because I do not really know enough about the specific matters he mentions. However, I can say that national identity cards are commonplace on mainland Europe and, in fact, the majority of member states of the European Union have identification systems. There is the provision in Article 87 of the GDPR for the processing of the national identification number. The provision states that member states may further determine the specific conditions for the processing of the national identification number or any other identifier of general application.

There is the possibility, which is foreseen and recognised in the General Data Protection Regulation, of having a national identification number. When it comes to legislation to give

effect to any of this, as I mentioned earlier, there will be an obligation in future to consult with the Data Protection Commissioner. The Data Protection Commissioner would be in a position to give advice to public authorities, whether Departments or local authorities, when it comes to either legislative measures or measures to give effect to legislative measures concerning data processing.

Deputy Mick Wallace: I wish to follow up on the points that Deputy Jim O'Callaghan and Deputy Jack Chambers made around all these compensation claims ending up in the courts. God knows, there could be many of them since the provisions are expanding beyond material damage. Does anyone in Europe deal with this through a data protection commission rather than automatically going through the courts? Does everyone in Europe have to do it through the courts?

Mr. Seamus Carroll: As far as I am aware, this is not typically the type of work that is done by supervisory authorities. Some supervisory authorities may already have the power to impose penalties, including administrative fines. However, when it comes to compensation, I am not aware that supervisory authorities have such power. This is typically the kind of work carried out by courts.

Obviously, there may be bodies such as the Injuries Board, which has a role. The Injuries Board has an adjacent role to the courts when it comes to awarding compensation. I do not have sufficient information on the position in other member states to say more.

Deputy Mick Wallace: The people with deep pockets are still going to be hard to beat when it ends up in court, are they not?

Chairman: That is a statement. I do not think it was a question.

Deputy Mick Wallace: It was a question, but he is not answering it.

Mr. Seamus Carroll: All I can say is that our existing case law and the interpretation of our existing legislation has confined liability to material loss. That has now been changed by this. There is, inevitably, the risk of extended or expanded compensation claims arising from this. This is all the more reason that those who process personal data need to gear up in advance of implementation in May next year.

Senator Niall Ó Donnghaile: I thank Mr. Carroll for his contribution. I am going to ask a hypothetical question, with the caveat that it is still outworking in my head. We have a unique situation here with Brexit and the North. Obviously, there is movement of people regularly across both sides of the Border, whether for hospital appointments or involving people using credit cards, downloading apps or signing up to tourism websites and so on. At present, they are all subject to European guidelines. We are heading into a situation where that may remain the case or it may not. My hypothetical question is around any exploratory work or research into scenarios involving someone in the North if the North is no longer subject to these guidelines. Such a person would remain an EU citizen and continue to attend hospital appointments, use credit cards and download apps. Are such people, as EU citizens, protected by this legislation? This might not only apply in the case of the North, but it might apply to another jurisdiction. Is there a danger that their information could then be shared, used or abused in a way that is not compliant with the legislation as laid out here?

Mr. Seamus Carroll: I thank Senator Ó Donnghaile. That is a really interesting and pertinent question. The position is that the UK will already have given effect to the General Data

Protection Regulation and the directive prior to Brexit. At the point of Brexit, the United Kingdom will be compliant with EU data protection law. Then, on leaving the EU, the United Kingdom will no longer be a member state. In that case there is a mechanism that is called an adequacy finding. This is based on a European Commission decision. We have heard about this in the past with regard to the safe harbour decision and, more recently, the privacy shield. Adequacy decisions already exist for Canada, New Zealand, Israel and numerous other third countries. Basically, it means that where the data protection arrangements of those third countries equate with those applicable within the member states, then transfers of personal data across borders can continue without hindrance.

A difficulty would arise if the UK were to adjust data protection standards post-Brexit. That would certainly raise the question of whether the applicable data protection standards within the UK were still at the same level as the EU standards. On the understanding and the assumption that UK data protection standards would remain equivalent to those in the European Union, one could expect an adequacy decision of the European Commission - which is provided for in the regulation - that would permit continued unhindered transfers of personal data into and out of the United Kingdom to the EU.

Chairman: Senator Ó Donnghaile, do you have any follow-up questions?

Senator Niall Ó Donnghaile: No.

Chairman: Thank you for that. Mr. Carroll, in the absence of any other hands showing I would like to ask some questions. Head 13 relates to attendance of the commissioner before an Oireachtas committee. We are going to have that opportunity shortly. Head 13 states: "The Commissioner or, in the event of more than one Commissioner, the Chairperson shall, at the request in writing of a committee of the Oireachtas, attend before it to give account for the general administration of the Commission and report on the performance of its functions." I take it this provision is referring to any committee of the Oireachtas. However, the explanatory note is quite specific in respect of accountability to an Oireachtas committee rather than to the Minister and Department and how it will serve to underpin the functional independence. In that instance - this is only for clarity, and no better place to ask for it - is the Oireachtas Joint Committee on Justice and Equality the designated committee in respect of the primary accountability of the commissioner or commission, as the case might be? Would she, he or they be open to requests from any committee of these Houses?

Mr. Seamus Carroll: Perhaps the statement is in a synopsised form. The intention is that the commissioner or chairperson of the commission could appear before any Oireachtas committee. This would include if or when the commission had a separate Vote and it would appear before the Committee of Public Accounts as well. I can confirm that this provision is not intended to refer to a single committee. Perhaps when the Bill is drafted, it will make that clearer.

Chairman: The head refers to accountability to an Oireachtas committee rather than to the Minister and Department. I take it that the Minister and the Department is not the broad church in that case. Is it particular to the Joint Committee on Justice and Equality as the primary reference point?

Mr. Seamus Carroll: I wish to confirm that the supervisory authority under the general data protection regulation and the directive must operate with complete independence. Therefore, the commission or commissioner, as is the case at present, is not accountable to the Minister or the Department.

Chairman: Yet the head refers to accountability to an Oireachtas committee to serve to underpin the functional independence of the commission. The relationship to the committee system is what I am trying to establish definitively. Perhaps the situation is not as I understood it to be. It may be wider and run across the full gamut of the committee structure.

Mr. Seamus Carroll: It would certainly include the Committee of Public Accounts to the extent that the commission would have a separate Vote and the chairperson or commissioner would be the Accounting Officer for that Vote. However, it does not preclude the commissioner from being called before other committees. Obviously, the Joint Committee on Justice and Equality is one such committee, but other committees may be interested in the views of the commissioner.

Chairman: My next question relates to heads 12 and 13. Head 12 relates to financial control. Of course it is a blank. I have before me the explanatory note. It is all in the context of financial control. The explanatory note relating to head 13 sets it out in a very different way, although it also relates to financial control. I wonder is there a need to streamline one or other of these. There seems to be a crossover in terms of the explanatory position.

Mr. Seamus Carroll: In so far as head 12 is concerned, we make reference in the head to the provision within Article 52 of the regulation which refers to a financial control mechanism which does not affect its independence. That is the underpinning motivation for having a separate Vote with the chairperson as the Accounting Officer.

Perhaps that thinking has been carried over here into head 13, but that is in the context of accountability to or appearing before the Committee of Public Accounts. It does not preclude attendance before other committees, such as the Joint Committee on Justice and Equality. That will be made clear in the final drafted text.

Chairman: I would expect that. As matters stand, I did not think it was.

Finally, in regard to backup data, nowhere at all throughout the entire document on the heads is there any reference to backup data whatsoever. My understanding heretofore was that it is excluded under the scope of subject access requests currently. Is that what is intended to continue or will there be address in relation to backup data in the Bill as the process proceeds?

Mr. Seamus Carroll: There is no distinction whatever drawn in the GDPR between personal data and backed up personal data and the obligation on data controllers is similar in relation to both current data being used and backed up data. Under existing law, there is a specific provision in relation to backup data but that distinction between current data and backed up data does not appear in the General Data Protection Regulation.

Chairman: Is Mr. Carroll advising me and the committee that backup data is not excluded from the scope of subject access requests currently?

Mr. Seamus Carroll: It is under our current law, but under the GDPR and future law, it will not be.

Chairman: I was correct in stating the current position.

On behalf of the committee, I thank Mr. Carroll, Ms Walsh and Mr. O'Riordan for their attendance here this morning and their engagement with the committee, and for, I have to acknowledge, as others have, Mr. Carroll's informative contribution which will no doubt assist the

committee in considering this issue.

The committee will now suspend to facilitate the arrival of our next witness.

Sitting suspended at 10.13 a.m. and resumed at 10.15 a.m.

Chairman: The purpose of this part of our meeting is to continue our scrutiny of the general scheme of the Data Protection Bill 2017. I welcome the Data Protection Commissioner, Ms Helen Dixon, who is joined by Mr. John O'Dwyer and Ms Anna Morgan. In the Gallery, I already acknowledged Ms Emily Burke. On behalf of the committee, I thank them all for their attendance here this morning. The format of the meeting with which they will be familiar is that the Data Protection Commissioner will be invited to make a brief opening statement and this will be followed by a question-and-answer session.

Before we begin, I must draw the attention of the witnesses to the situation in relation to privilege. Please note that witnesses are protected by absolute privilege in respect of the evidence they are to give to the committee. However, if they are directed by the committee to cease giving evidence on a particular matter and they continue to so do, they are entitled thereafter only to a qualified privilege in respect of their evidence. They are directed that only evidence connected with the subject matter of these proceedings is to be given and they are asked to respect the parliamentary practice to the effect that, where possible, they should not criticise or make charges against any person, persons or entity by name or in such a way as to make him, her or it identifiable. Members should be aware that, under the salient rulings of the Chair, members should not comment on, criticise or make charges against a person outside the House or an official either by name or in such a way as to make him or her identifiable.

I invite Ms Dixon to make her opening statement.

Ms Helen Dixon: I thank the Chair and the committee for this opportunity to engage in relation to the published general scheme of the Data Protection Bill 2017. As indicated by the Chair, I am joined this morning by two deputy commissioners from the Data Protection Commission, DPC. These are John O'Dwyer, who heads up the investigations function, and Anna Morgan, who heads our legal advisory function. I do not intend to read out the full written opening statement that I submitted to the committee but rather to briefly highlight for the committee the key issues that were presented in that statement. I trust that is in order for the committee.

This committee will be aware that data protection law is now being subject to a once in a generation overhaul and modernisation. In a recent opinion of the Advocate General, Mr. Bobek, at the Court of Justice of the European Union, he pointed out that there is no doubt that the protection of personal data is of primordial importance in the digital age and he went on to reflect the main concern of personal data protection, for which it has been originally introduced and must be vigorously protected: large-scale processing of personal data by mechanical, digital means, in all its varieties, such as the compiling, administration, and the use of large datasets, passing on of datasets for purposes other than legitimate ones, assembling and harvesting of metadata, and so on.

Since the existing data protection directive was implemented in the EU in 1995, every organisation has now essentially become a technology organisation and a digital data organisation, not to mention the growth of the true born-on-the-Internet companies. Every Department typically has a website and a range of databases. Almost any corner shop operates a till and pro-

cesses credit card payments electronically, for example. The laws, therefore, required updating to allow for the scale of technology developments and to cover the important case law that has issued in recent years from the CJEU interpreting the fundamental right in Article 8 of the EU charter to have one's personal data protected.

In rendering the law fit for today's purposes and in seeking to ensure innovation is not stifled but happens in a way that respects fundamental rights, the EU is also overhauling the role of data protection authorities under the law, in particular, applying a much harder enforcement and sanctioning edge to our role. Europe's law makers have taken the view that infringements of data protection law are a serious matter and are demanding more accountability and transparency from every organisation that processes personal data, backed up by strong *ex post* enforcement by data protection regulators.

As the Department of Justice and Equality outlined this morning, the structure of the new laws that will apply in Ireland from May 2018 will be in the following form. The committee has received copies of the direct effect General Data Protection Regulation, GDPR, text from us yesterday. This forms the substance of the new data protection law in Ireland from May 2018 and it is intended to be implemented as one harmonised law across the European Union, EU. In addition to the direct effect GDPR text, there will be an Irish data protection Act, and that is the subject of our discussions today. It will implement a limited number of measures to give further effect to some of the provisions in the GDPR and transposes, as we heard, the law enforcement directive that will come into effect in May 2018. In due course, we will also have a new e-privacy regulation that will apply with direct effect and it will govern confidentiality of communications and e-marketing.

In general terms, the Data Protection Commissioner, DPC, welcomes the new legal regime for data protection law and the important additions to our tool kit as an enforcer. It is undoubtedly the case there will be investigations where a punitive fine is warranted in order to deter organisations from failing to invest in compliance and to deter them from creating risks for consumers and individuals. As a supervisory authority, we occupy a unique position in Europe in that our supervision remit covers the largest global Internet companies that have their European bases here in Ireland. As a result of the platform types they represent and the volume of users they service at a scale of hundreds of millions, a comprehensive tool kit as an enforcer is a necessity. The DPC is extremely pleased that Ireland is now one of the first countries in Europe to publish heads of a Bill to underpin the GDPR. It facilitates greater planning by organisations preparing for the GDPR to have some insight into how the new Irish Act underpinning the GDPR may be structured. However, there are three key areas to which we want to bring the committee's particular attention.

The first is the matter raised earlier by the Department of Justice and Equality relating to the retention of portions of the existing data protection legislation. As was noted earlier, it is intended that when the GDPR comes into direct effect in May 2018, the existing EU 1995 directive 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. However, as we heard from the Department of Justice and Equality, there is no guarantee presented in the heads of Bill that were published that the existing Irish Data Protection Acts from 1988 and 2003 will be repealed. 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. The Irish DPC is of the view that if the pieces of the 1988 and 2003 Acts to be retained 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.

The second matter we wanted to raise relates to administrative fines for public authorities and bodies. It is a serious matter of concern for the DPC under the general scheme, which relates to head 23, that it is proposed that administrative fines would not be imposed on public bodies and authorities. The 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. Additionally, the workload proposed for the DPC in making assessments of whether public bodies are engaged in activities that would compete with equivalent private sector bodies takes us away from our substantive role in data protection terms.

The final issue we wanted to bring to the attention of the committee relates to the handling of complaints from individuals under the GDPR, which introduces changes in 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 from 1988 and 2003, an individual has the statutory right to seek a decision or determination from the Data Protection Commission in all complaints or cases where a complaint has been made to the DPC about a data controller or processor where the complaint could be amicably resolved. The GDPR takes a broader approach, envisaging outcomes to complaints other than formal decisions. For example, it envisages the provision of guidance or information to the complainant to self-resolve a complaint. 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 the complaint handled and be informed within three months on the progress or outcome of the complaint. It is also important to note in this context that the supervisory authority is required to investigate a complaint to the extent appropriate. Our aim in these circumstances will be to ensure our resources are deployed in a way that maximises them and pursues investigations in the areas of the most grave and enduring infringements on an objective and priority basis.

I thank the Chairman and members of the committee for their attention and we look forward to answering any questions the committee might have.

Chairman: I thank Ms Dixon. I will call members in order and a nod to the Chair will suffice.

Deputy Jim O'Callaghan: I thank Ms Dixon for her presentation and I agree with her when she states it would be beneficial to have a consolidated piece of legislation setting out the laws in respect of data protection, as opposed to having three different pieces of legislation that we would have to check for consistency. The witness mentioned it might be worthwhile if a process could be done whereby somebody could go back through the legislation to identify the parts of the 1988 and 2003 Acts that need to be retained. Does Ms Dixon see her office having a role in identifying what needs to be retained?

Ms Helen Dixon: No, it would not be a process for our office. Our understanding is the reason for doubt about repealing the 1988 and 2003 Acts in total is the 1988 Act in particular transposed our Convention 108 obligations under the Council of Europe. They stray outside the areas of competence of the EU. For example, supervision in the area of national security will be required under Convention 108. In order to retain pieces of the 1988 and 2003 Acts, the Department must identify those pieces. In the course of doing that it seems it would be open to fully repeal and rewrite those small pieces, *de novo*, into a new Act.

Deputy Jim O'Callaghan: The office will come to impose administrative fines but what parameters will it work from? Are there regulations or restrictions concerning what type of fines can be imposed?

Ms Helen Dixon: The GDPR provides for an ability for us to impose sanctions and fines. The type of sanctions we can impose are warnings and we can issue enforcement notices requiring rectification and so on. Under Article 83 of the GDPR, there is a presumption that where there is a sanction in contemplation and we have identified an infringement such that a sanction is in scope, Article 83 provides for the presumption that it will include an administrative fine. With regard to such administrative fines, in the case of the most serious infringements they can be up to €20 million or 4% of the global turnover of undertakings. There is some discretion in terms of the administrative fines we can impose. With regard to Article 83 of the GDPR, it sets out that initially we would look at whether a sanction is in scope in terms of the infringement that we are looking at; we would assess that based on the gravity and duration of the infringement. Then it provides for a range of criteria that we would take into account as mitigation factors in terms of the quantum of the fine we would impose, so there is some prescription in the GDPR for how we would go about that process.

Deputy Jim O'Callaghan: Am I correct that, at present, if somebody wishes to make a complaint about their data being abused, he or she can go either to the Office of the Data Protection Commissioner or to court? It appears from what the Department says that the only way one can get compensation is by going to court. Are there difficulties in permitting a parallel process such as that? Does the witness think that people who have a complaint should, in the first instance, be forced to make a complaint to her office?

Ms Helen Dixon: There has always been an interesting position in terms of the role of data protection authorities in Europe. Mr. Carroll alluded to this. We are currently, and will not be in the future under the GDPR, full blown ombudsmen. Currently, in investigating complaints we do not have the powers to order redress or to deliver compensation. That position is retained under the GDPR. Currently, section 7 of the Data Protection Act provides that individuals can go to court to seek compensation if they consider that they have suffered damage but, as per FBD *v.* Collins, it must be material damage. It is expanded under Article 82 of GDPR, whereby individuals can go to court to seek compensation for material or non-material damage. Our reading of the GDPR is that it is prescriptive that court proceedings are required to achieve that compensation. I do not believe it is envisaged that there could be a parallel process.

Deputy Jim O'Callaghan: Finally, does the witness think there will be a considerable increase in the workload of her office when this legislation is enacted? To what extent does she think the office's resources will have to be enhanced on foot of the enactment of the legislation?

Ms Helen Dixon: We certainly envisage an increase in workload. We believe this will arise in a number of ways. As Mr. Carroll outlined earlier, we have a broader range of powers and functions under the GDPR. We believe the increased workload will stem primarily, we hope,

from greater awareness of individuals and data subjects of their rights under EU legislation. Once obligations fall under the GDPR on all sorts of organisations to be more transparent and accountable with data subjects, awareness of and concern about their rights will increase. We believe we will start to see more complaints. In addition, data subjects are acquiring new rights under the GDPR. They are acquiring rights of data portability in certain cases, so we will see new types of complaints starting to arise requiring new technical expertise on our part. In addition, our supervisory role relating to all of the organisations we supervise will increase. As there are new accountability and transparency requirements on organisations we will be required to supervise that they are implementing those and in far more prescriptive terms than we are required to do currently.

Another area where we envisage our workload increasing relates to the cross-border processing cases with which we will have to deal. As a supervisory authority, we will act as the lead supervisory authority in Europe for all of the Internet multinationals located here. When we investigate a matter relating to one of those companies, we are obliged under the GDPR to consult with our fellow data protection authorities in Europe, take utmost account of the views they express on the matter and, ultimately, if we cannot incorporate their views into the findings we make we will be obliged to refer the matter to the new European data protection board which will make a decision as to whether an objection from another data protection authority is relevant and reasoned. Where it finds that the objection is relevant and reasoned, the European data protection board will then take a decision in the case. There is an entirely new set of mechanisms, complexity and layers. We are not exercising exclusive competence under Irish data protection Acts any longer, but will be implementing this harmonised regulation.

We anticipate an increased workload across a range of areas. There is also the requirement for data controllers to notify breaches to us on a mandatory basis, which will massively increase the number of breaches notified to the authority and which will require subsequent investigation. It is also required of data controllers who are obliged to appoint a data protection officer to notify those details to us. There is a range of areas where we have new functions, in addition to the prior consultation function with the data protection authority where new legislation is to be implemented. Where any type of data controller has been obliged to conduct a data protection impact assessment and has been unable to mitigate all of the risks they are obliged to consult with the data protection authority. The Deputy is correct that we will need many more resources to implement the GDPR.

Deputy Mick Wallace: I thank the witness for her presentation. Article 51 of the GDPR requires member states to establish an independent authority to monitor and enforce the GDPR. Under the new Bill, the Office of the Data Protection Commissioner will be reconfigured as a data protection commission which, depending on the workload, may be assigned more than one commissioner. In 2016, Digital Rights Ireland commenced legal proceedings against the Irish State challenging the independence of the commissioner and alleging that the commissioner did not effectively monitor databases containing personal data that had been created by public bodies. Also, the fact that the commissioner is integrated into the Department of Justice and Equality and that many of the employees of the office are civil servants might raise serious questions about the independence of the office. Under Article 52.6 of the GDPR, the supervisory authority, the data protection commission, must be subject to financial control which does not affect its independence and must have separate public budgets. However, head 12 of the general scheme of the Bill, entitled "Financial control", is blank. Is there any clarity as to how the Government plans to ensure the independence of the body and that it will have a separate public budget? I will put my second question presently.

Chairman: Does Ms Dixon wish to take that question first?

Ms Helen Dixon: The Deputy is correct that head 12 is blank at present. Our understanding from Mr. Carroll's presentation earlier and from discussions with him is that this matter is still under consideration. He outlined that one proposal is to make the chair of the Data Protection Commission or the Data Protection Commissioner an Accounting Officer who would account directly to the Committee of Public Accounts. There is debate as to whether that is necessary to achieve the level of independence required. For example, at present we have a ring-fenced budget and we have full discretion to decide how we spend and deploy it. That is where the area of remaining debate lies. With regard to our view, we are open to advice that either will suffice to serve to underline our independence. There probably is a benefit in being our own, stand alone, Accounting Officer in terms of perception.

Deputy Mick Wallace: We see a pattern of the Government being keen to keep a firm hand on organisations. For example, in the case of the Garda Síochána Ombudsman Commission, GSOC, which we would argue was designed to fail, it made sure it failed by giving it as little money as possible. How effective will the commission be if the Government pulls its strings too closely?

On a separate issue, I heard the Minister for Public Expenditure and Reform, Deputy Paschal Donohoe, defending some of the big brother type policies around the collection of data as an issue of State security and using the threat of terrorism as a good reason for these policies. There will always be a conflict between the individual and how much data the State wishes to store on the individual, and the State will use State security as a reason. I raised the issue of telephone tapping when Vodafone tapped into the fibre optic cable off the coast of Wales a couple of years ago, which gave it access to almost every telephone in Ireland at the time. It was impossible to get answers from the Government about it. We do not know why. It was also impossible to get information back from it as to what it knew about the situation. Was it legal? Would the decision come from Government Communications Headquarters, GCHQ? The Government seems to hide behind this State security thing in order to do what it likes in this area. Only a couple of weeks ago, or last week, we heard the British Prime Minister, Theresa May, make the argument that human rights could almost be undermined in the interest of security, to fight terrorism.

Is there going to be a battle of that nature here, around how our data is being stored and how much information authorities are going to be allowed to put together on us? I asked Mr. Seamus Carroll last time and he did not really want to give me an answer on it. Are we entitled to know what authorities put down about us on this identity card or our passports?

Ms Helen Dixon: The Deputy is correct that there will always be tension between security and liberty, and the need for surveillance, interception, and intelligence versus protection of fundamental rights. The case law from the European Court of Justice has been very instructive in this area. The Deputy will be familiar with the fact that it struck down Europe's data retention laws in 2014 and it outlined, in striking down the data retention laws in Europe, a test for necessity and proportionality. In particular, it pointed out that there cannot be mass and bulk scale collection. It requires to be targeted and there needs to be evidence as to the necessity and proportionality. That gives us clues as to how the Court of Justice interprets data protection laws *vis-à-vis* this issue. First, evidence, necessity, and proportionality need to be demonstrated. There needs to be protection of rights of individuals to be notified when they are the subject of surveillance or interception.

We are aware that the Department of Justice and Equality is looking at modernising the surveillance and interception laws in Ireland. We are strongly of the view that it needs to look at strengthening the oversight mechanisms that are in place. As the Deputy knows, under current interception legislation, the Minister for Justice and Equality can sign off on an interception request. There is currently no judicial oversight of that process. There is a definite need to look at modernising those laws with regard to reacting to the threats that countries are now exposed to, but there is also a need at the same time to look at what the oversight in that area is. When Mr. Edward Snowden made his disclosures in 2013, he kicked off a very important debate on this whole area with regard to how certain intelligence agencies in the US were operating. It is an extremely important area in which we have to actively participate, and we are doing so.

On the question the Deputy asked about whether each of us is entitled to know what data is encoded on any identity card to which we are subject, we are entirely entitled to know. We have a clear right under current data protection legislation and under future data protection legislation to know precisely what fields of data about each of us are recorded on that card. It should not need to be something that one would need to submit a specific access request to obtain. What is encoded on that card should be readily known to a person at this point. That really points to an issue with transparency with regard to implementation of what is being rolled out.

Deputy Mick Wallace: On the same subject, are phone operators obliged to tell us if anyone has asked them for access to our communications?

Ms Helen Dixon: There is no specific provision to that effect in the Communications (Retention of Data) Act 2011. It puts obligations on the telecoms companies to provide metadata about individuals when they receive appropriately authorised requests from certain bodies that are proscribed under that data retention legislation, such as the Revenue Commissioners or An Garda Síochána. There is no specific provision that sets out an obligation for them to notify any individual who is the subject of such a request. However, under general data protection legislation, it is open to any individual to make an access request seeking a copy of his or her personal data from a telecoms company or any other organisation. That may be a means by which it could be pursued in general terms.

Deputy Mick Wallace: I have one last question. At present, a garda above the rank of superintendent can give permission to a lower-ranked garda to monitor a person in some ways related to communications. All these things do not have to go through the courts or the Minister for Justice and Equality. I presume Ms Dixon is aware of that. Does she think it is right that gardaí do not have to go to court for that?

Ms Helen Dixon: I am not aware of the specific-----

Deputy Mick Wallace: For example, if gardaí wanted to put a tracking device on a vehicle, they do not have to go to court to get permission. Anyone above the rank of superintendent can give permission to a garda of a lower rank to go ahead and do it. They do not have to go through the courts to do it.

Ms Helen Dixon: In any case like that, which clearly constitutes a very significant interference with privacy rights, the structure for signing off on such a request is important. It is much more important to first look at what the legal basis for conducting such monitoring would be. How is it legitimised under data protection law? Is it absolutely necessary? Is there a means of obtaining the same results without interfering with privacy rights in that drastic way, etc.? We would have to look at any specific case and examine whether the full analysis has been

conducted in order to legitimise it under data protection law.

Deputy Mick Wallace: Under the current system, the judge undertakes a one-hour review of all the cases for the year at the end of the year, and it is an outrageous arrangement. There is absolutely zero transparency and accountability for how that operates. Is that outside Ms Dixon's field or does it fall within her remit?

Chairman: I ask that this be Ms Dixon's last response.

Ms Helen Dixon: We are responsible in general terms for supervising all bodies, both public and private sector, in Ireland. That includes enforcement authorities. It is within our remit to supervise any area of bodies' processing of personal data, and if an area of risk, such as what the Deputy may be outlining now, comes to our attention, it is at our discretion to focus our resources in examining it.

Senator Frances Black: I thank Ms Dixon for her very clear and precise presentation. This is not an area I am familiar with, and I appreciate her coming in today to give a good explanation of what it is all about. I think the legislation is very positive. I imagine it is also a minefield. What does Ms Dixon think are going to be issues? Resources are obviously one. What other challenges does she think there are with this legislation going forward?

Ms Helen Dixon: I will have to limit myself. It is full of challenges. Significant challenges with the new data protection regime relate to this issue that I mentioned of so-called cross-border processing of data, for example, processing of data by Internet multinationals located in Ireland, where the data of all Europeans is processed. In those cases, we will not be exercising our own exclusive competence. We are required to co-operate with other European data protection authorities and to keep them informed of investigations as we conduct them, and of the outcome, and to allow them to express views which we are required to take account of. It is a significant complication when one is trying to co-ordinate across such a range of data protection authorities with very different cultural backdrops to how they view data protection in general terms, but also how they view, for example, American corporations that target services at European users. We anticipate this is going to create a layer of complexity as we become involved in bringing decisions before the European Data Protection Board.

I did not mention earlier, because it is probably a level of complexity too far, that once the European Data Protection Board makes a decision there will be a further layer of complexity in how those decisions can be appealed, such as through annulment actions before the European Court of Justice. This is a very particular challenge. An ongoing challenge in data protection legislation is that it is high level and principles based, as will be future laws to large extent. This is appropriate because the laws need to offer a level of flexibility to all of the various organisations to which they apply. We find there is a challenge, in particular for public sector bodies, in implementing principles-based legislation because it means they need to step back and conduct detailed analysis in every scenario that presents, in terms of processing personal data, looking at whether there is a statutory basis to collect and process it in the first place, whether it is meeting the legitimising conditions and whether it is meeting the transparency requirements to users, and then deciding whether all of this amounts to a lawful purpose. It is the challenge of encouraging organisations to conduct this analysis themselves rather than expecting a simple binary answer on whether they can do something or not.

Senator Niall Ó Donnghaile: I thank Ms Dixon for her presentation and I apologise for missing the first part. I want to reiterate the question I put to Mr. Carroll this morning and ex-

pand on it slightly. I appreciate this is hypothetical, and nobody likes dealing in hypotheticals, but we are where we are in this regard. It is on what the impact of Brexit might be, given our unique circumstances. The British Government is committing to the General Data Protection Regulation, GDPR, and retaining existing EU legislation, directives and regulations. If it was to divert from this at a later stage, or amend or distort it down the line, is exploratory work being done on how this would impact the retention and sharing of data of EU citizens in a jurisdiction which is no longer in the EU? A large number of people in the North are EU citizens, and will remain so regardless of the outworking of Brexit.

Another issue came to me as we have been sitting here, because people are following the meeting on social media and I have received a few tweets. Small and medium businesses retain data as part of their work, and there is a huge degree of uncertainty on both sides of the Border about insurance and how the change in legislation will impact on them in this regard. I caveat all of this with the appreciation that it is a hypothetical situation, but I want to pick Ms Dixon's brain and get her initial views.

Ms Helen Dixon: The question is very clear. As Senator Ó Donnghaile is aware, data protection law starts out with a prohibition on the transfer of personal data of EU persons outside of the EU, as will future law under the GDPR. The obvious consequence of Brexit when it happens is that the UK will become a third country for the purpose of the transfer of data, which is what the Senator has referenced. As Mr. Carroll outlined, in circumstances where the UK is no longer implementing the GDPR and is no longer party to it, it remains to be seen whether it will retain an equivalent set of standards, something that effectively mirrors the GDPR. In these circumstances, we anticipate the UK would apply for an adequacy finding of the EU Commission. As Senator Ó Donnghaile knows, once the EU Commission makes an adequacy finding in respect of a third country it effectively covers transfers, subject to ongoing review by the EU Commission that it is retaining the standards. The ultimate solution is that the UK would retain laws equivalent to the standard under the GDPR and the EU Commission would make an adequacy finding.

If it is the case the Commission does not make an adequacy finding there will be costs for business in terms of legitimising the transfers of personal data between Ireland and the UK, because one of the legal mechanisms provided for under the law would have to be implemented to effect the transfers. The types of legal mechanisms provided for are binding corporate rules or standard contractual clauses. These are means by which an entity can adduce adequate safeguards, as it is described in the law. There is a legal cost to implementing these types of mechanisms. It is the case that transfers will be capable of being affected post-Brexit, but it remains to be seen as to whether this will have to be achieved with a cost to business in terms of how it will implement the transfers.

Chairman: I welcome Deputy Buckley to this meeting of the Oireachtas Joint Committee on Justice and Equality. I take it he would like to pose a question to the commissioner.

Deputy Pat Buckley: I thank the Chairman for giving me this opportunity. My question is on the psychologists, psychiatrists and counsellors. The best example I can give is filicide, as in murder-suicide where someone's spouse takes their children and kills them as well as himself or herself. Is there any way of adjusting, through impact assessment studies or another solution, whereby if an individual, male or female, is attending a counsellor, psychiatrist or psychologist and there is a flag that the person may be a threat to family members the information could be disclosed to the person's partner, male or female? I have been approached on a number of occasions by spouses who have survived but have lost family members to suicide. They are

extremely frustrated. They feel that if some of the information had been disclosed they could have had an opportunity to protect their children.

Chairman: Deputy Buckley has been involved in suicide prevention counselling for a number of years. I can understand the relevance of his question.

Ms Helen Dixon: It is a very interesting question. As we frequently point out as a data protection authority, data protection law does not prohibit policy choices by the Government. It does not necessarily prohibit any activity. What data protection law does is prohibit the processing of personal data unless it can be justified and legitimised under the data protection laws. Data protection law should never be used to obfuscate what is correct to do in all of the circumstances. Under data protection law, of course disclosures of any individual's personal data, particularly his or her sensitive health-related personal data and personal data relating to mental health, is prohibited unless there are specific circumstances that would justify it. Personal data can be disclosed where it is necessary to save a life or prevent serious harm to an individual. Each individual case would have to be looked at to see whether a basis exists to make such a disclosure. It is also likely to be the case that in circumstances such as those outlined by the Deputy, data protection law may not be all that is in scope, and he knows this better than I do. There may be medical ethical issues at play. In general terms, data protection law does not prevent what needs to be done to save the life of any individual.

Deputy Pat Buckley: I thank Ms Dixon for her answer. I wanted clarity, and I thought the best people to ask were those at the Office of the Data Protection Commissioner. I appreciate the answer and thank Ms Dixon very much.

Chairman: I have several questions, based on my experience as an elected representative over a number of years and the areas that have been most often reflected to me. I also have a background in banking and issues have been raised by a number of people, even within the employ of our banking institutions, but more particularly those who have been most seriously affected by the significant downturn in the economy and have not been able to maintain their repayment schedule in regard to house mortgages or whatever. My point relates primarily to the house mortgage area, but nevertheless we are also talking about serviced accounts. They are not completely abandoned. People present to a banking institution and proffer significant personal data and information in order to secure a loan facility. What we have seen over recent years is what is described as a significant sell-off of a body of negotiated mortgages loans to third party banking institutions, and not always within this jurisdiction. Sometimes they are domiciled outside the jurisdiction, but some have a representative office and nothing more.

It is not just the loan that goes or the fact that there is a balance outstanding that has to continue to be serviced. It is all of the respective data in regard to the borrower. Instances have been brought to my attention where significant upset has been caused in terms of information on the individual, the family, those in a position to make an input into helping to address an outstanding balance and other members of a family who have come on board to help. These cases have presented where that data regarding not even the principal borrower but other members of their family who have come on board to assist have been given out to new anchor lenders in regard to the borrowing facility. Is there any prohibition or is anything envisaged in terms of the pending legislation that would prohibit this activity, which has been happening wholesale over the past number of years and has caused grave upset for many people?

Ms Helen Dixon: It is a complex question that stems from the terms of any mortgage individuals take out with the bank and the terms and conditions set out in the mortgage, which

may provide for the selling on of the loan to another provider. In terms of the transfer of data, that would have to be based on a necessity of the transfer of data and underpinned in the terms of the mortgage. Before commenting on that, therefore, we would need to look at any specific case regarding the terms of any given mortgage and the personal data that transferred in regard to any transfer of the loan.

Chairman: That is in terms of the specifics of any particular case, but in the broad brush stroke circumstance, if somebody goes in to their local banking institution, whatever representative office it may be, they believe they are dealing with whomever. The entire situation has changed enormously. They end up dealing with a body, an institution or a financial house that they never heard tell of before and that have no public persona whatsoever. They never get to meet an individual yet these people are in possession of all their relevant data that was proffered to the initial lender in good faith for the purpose of securing the loan, and they can go off and market it subsequently. In broad brush stroke terms, is there anything that can be done to address that?

Ms Helen Dixon: As I said earlier to Deputy Buckley, data protection law will not pass a view on whether, in general terms, it is a good or a bad thing that lenders can sell on loan books in this way. Data protection law is looking at whether there is a legal basis for the transfer of the personal data and whether clear and accurate notice is given to any individual who took out a loan that the loan could be called in at some point or sold onwards to a third party and that at the time of the selling on of the loan book, clear notice is given to the individual of the data that is transferring and to which new data controller. We would have to look in the round at whether in a specific case we would outline that clear notice was given to an individual taking out a loan and that this was an eventuality.

Chairman: There is work to be done in that area.

I have a final question. I refer to the consequences of the General Data Protection Regulation, GDPR, coming into play in regard to the respective roles of Members of both the Dáil and the Seanad. Any number of questions have been posed by Members as to whether they need to appoint a data protection officer. What is our respective position regarding the outworking of the new legislation? A raft of different questions have been posed. As representatives of the people who are meeting with members of the public on an almost daily basis and taking detailed personal information to assist them as a chosen representative in whatever particular case they want assistance, from the questions posed, even in terms of the current position, never mind the changes envisaged, it would be very helpful if some briefing could be prepared for Members of the Houses of the Oireachtas, many of whom are new Members since last year. The questions posed are reasonable. The proposal would be either to have Ms Dixon's office issue a briefing to the Members of both Houses or at some point in time, whether it is post or prior to the passage of the legislation - it is a call of its own choosing - to come here and brief Members of the Dáil and Seanad on the impact of the consequential outworking of the new legislation with regard to their roles and responsibilities. How would Ms Dixon respond to that?

Ms Helen Dixon: That is a very helpful suggestion. We would be very pleased to come in at any point and make a presentation. We are extremely pleased to hear that there has been some consideration by Members of the Oireachtas of the way the new law applied to them. It would be useful to receive some of the questions they are hearing in advance. We have a dedicated email address, *oireachtasatdataprotection.ie*. Questions could be submitted to that email address, which would help us in drawing up guidance but also in preparing a presentation that addresses the kinds of issues about which Members of the Oireachtas are concerned. The

Chairman is correct. They are considerable processors of personal data and sensitive personal data. We would be pleased to assist in giving guidance as to which provisions in particular apply and how they apply.

Chairman: I thank Ms Dixon for that. As there are no other outstanding points to be made, on behalf of the committee, I thank the commissioner for her engagement with the committee and her very informative contribution. I thank Ms Morgan and Mr. O'Dwyer for their attendance with her today, and Ms Burke in the Visitors Gallery.

That concludes our consideration of the Data Protection Bill for today. We will resume and engage with other parties coming before the committee over the coming weeks. We hope to conclude before the summer recess. The meeting will be suspended to facilitate the commissioner and her team to leave.

Sitting suspended at 11.10 a.m. and resumed at 11.15 a.m.

Scrutiny of EU Legislative Proposals

Chairman: The purpose of this part of the meeting is to conduct further scrutiny of COM (2017) 252 on work-life balance for working parents and carers. I welcome Mr. Deaglán Ó Briain and Ms Jennifer O'Farrell from the Department of Justice and Equality. On behalf of the committee, I thank them both for their attendance today to discuss this proposal. The format of the meeting is that the witnesses will be invited to make a brief opening statement, and this will be followed by a question and answer session.

I am obliged to also give a reminder on privilege. Witnesses are protected by absolute privilege in respect of their evidence to this committee. However, if they are directed by the committee to cease giving evidence on a particular matter and they continue to do so do, they are entitled thereafter only to qualified privilege in respect of their evidence. They are directed that only evidence connected with the subject matter of these proceedings is to be given and they are asked to respect the parliamentary practice to the effect that, where possible, they should not criticise nor make charges against any person, persons or entity by name or in such a way as to make him, her or it identifiable. Members should be aware that, under the salient rulings of the Chair, they should not comment on, criticise or make charges against a person outside the Houses or an official, either by name or in such a way as to make him or her identifiable.

I invite Mr. Ó Briain to make his opening statement.

Mr. Deaglán Ó Briain: I thank the Chairman and members for the opportunity to address the committee. The Chairman has already introduced my colleague, Ms Jennifer O'Farrell, and we are both in the equality division of the Department of Justice and Equality, with responsibility for various equality issues, including family leave legislation. The Commission's proposals are directed at the area of family leave. We will endeavour to answer any questions the committee may have but our capacity to do so is limited on the basis that we are still at a very preliminary stage of examining this proposal and we do not have a Government position. Some considerable policy issues must be addressed before we arrive at a Government position. We do not yet have firm information on costs and other impacts and that is work in progress. We do not have Government guidance on the various policy issues but we will seek that Government guidance and a negotiating mandate once we finish our preliminary analysis in conjunction with

colleagues in all other relevant Departments.

We have supplied two scrutiny notes that we prepared for the committee on the related initiatives. One is a package of non-legislative and legislative measures to promote gender equality in the workplace and work-life balance. The second, within that, is the legislative proposal itself. The Commission's communication sets out details of an initiative that is being developed by the Commission to address the following challenges. These are the under-representation of women in the labour market across the European Union due to family responsibilities, such as responsibilities as a parent or carer of family members; the persisting pay gap between men and women, as well as an increasing pension gap that often leads to social exclusion and increased risk of poverty for women; and the failure of existing policies to bring equal opportunities for fathers and mothers with regard to labour market opportunities and treatment at work. That is the rationale expressed by the Commission for this package of measures.

Specifically, the Commission's objectives are to increase female participation in the labour market and reduce the gender pay gap, including elements of pay and pensions. It also intends to give workers more opportunity and choice in balancing their professional and care responsibilities by updating and modernising the current legal and policy framework, with particular attention to the role of men. The proposal is to support member states' modern family policies, including by addressing demographic and societal challenges and shortcomings in care service facilities and to eliminate economic disincentives to work for second earners who have family care responsibilities. The non-legislative actions proposed by the Commission are summarised in the scrutiny note and I do not propose to set them out. They pose no difficulties for us and we can, in fact, welcome and support this package of non-legislative actions.

As indicated in the scrutiny note, the legislative measures proposed follow on from the former maternity leave directive which was published by the Commission in 2008. The Commission withdrew the proposal as it had become clear that an impasse had been reached between the Council and the Parliament which could not be broken. There was also a case for a broader approach which was not focused solely on maternity leave to address work-life balance issues. During the Irish Presidency the then Minister of State, former Deputy Kathleen Lynch, tried to negotiate an end to the impasse but the distance between the parties was too wide and we were unable to broker a way forward in the time available to us.

The specific objectives of the directive now proposed are to improve access to work-life balance arrangements and increase the take-up of family-related leave and flexible working arrangements by men so as to promote greater gender equality in the labour market, including in relation to the gender pay gap and lifetime pension entitlement accruals. The following new elements are proposed. First is the possibility of flexible uptake, piecemeal and part-time, of the four-month entitlement to parental leave which would be paid at sick pay level. The four-month entitlement can be taken up until the child reaches the age of 12 years and cannot or would not be in the context of the Commission's proposals transferred between parents. Currently, we have a provision which is rooted in an EU directive for unpaid parental leave. The substantial change is that the leave would be paid. The proposal includes an entitlement to ten working days of paternity leave when a child is born, paid at sick pay level. As the directive sets out minimum standards, it is always possible for member states to go beyond them. The proposal also includes an entitlement to five days of carer's leave, paid at sick pay level, per year per worker to take care of seriously ill or dependent relatives and a right to request flexible working arrangements to take care of children up to 12 years old and for workers with caring responsibilities.

The Commission's proposals are being examined in detail. Some elements of the proposed directive pose very little difficulty for Ireland. We introduced two weeks' paternity leave last year; that is something we have and to which the Commission's proposal would make no difference. Our own policy direction domestically of moving to significantly expand paid leave to parents to cover the first year - a programme for Government commitment - is a very important context for us in addressing or examining the Commission's proposals. The scrutiny note we have provided comments on each of the elements. For now, rather than to repeat all of it, I draw attention to the proposal to change the current unpaid leave to paid leave. This would be the major new element for Ireland and needs very careful consideration from cost and impact on employment perspectives.

In coming to our assessment of the implications of the proposed directive, the first point to make is that we are conscious that previous EU gender equality initiatives have had a transformative impact on the position of women in Irish society. On that basis, we welcome in principle the Commission's initiative in presenting this package of proposals. This is subject to the normal detailed scrutiny, especially of those elements that are different from our current family leave regime and that could have significant cost implications. From an Exchequer perspective - this is a point that will, no doubt, be emphasised by our colleagues in the Department of Public Expenditure and Reform and other Departments - any additional cost would need to be met from a strictly limited fund available for each annual budget, the so-called "fiscal space". We also need to consult and negotiate on the detail with our European partners in due course, as well as with domestic stakeholders, including employer and employee representatives, in order that we fully understand the cost and other implications, particularly in the employment sphere.

What will happen next? We have an *ad hoc* interdepartmental advisory committee which has been set up to help us to analyse and cost the Commission's proposals. As it happens, the committee is due to meet tomorrow afternoon for the first time. We expect that its work will be completed quickly and that we will be able to seek a Government decision on our negotiating mandate before the summer break. We understand the Estonian Presidency is planning to organise a preliminary discussion on the file at ministerial level in July and that negotiations will commence in earnest in September. To reiterate, we are still at a very preliminary stage of our analysis and none of the key policy decisions on our negotiating position have yet been taken. There is a bit of work to be done before we make a submission to the Government. It will include consultation with employer and employee representatives which the committee may also be contemplating. Clearly, we will also reflect on the feedback from the committee. We will also consult colleagues in other Departments who have operational responsibilities in the social welfare system or as major employers within the public sector. Notwithstanding that rather serious limitation on what I can offer the committee by way of evidence, we will endeavour to address questions members have.

Chairman: I thank Mr. O'Briain. We have received submissions from ICTU, Ibec and the Departments of Social Protection and Jobs, Enterprise and Innovation. Our numbers are depleted this morning as there is an impending election in the Dáil Chamber and there is a lot of scurrying going on.

Deputy Jim O'Callaghan: I thank the officials for attending. This is obviously an important and significant proposal. Looking at the objectives of the proposed directive, they appear to be ones most Members of the Oireachtas would support. The obvious concern, however, is the total cost involved. While that is obviously a matter for another day, it is welcome that it is one that is on our radar at this early stage. It is something of which we will keep ourselves

apprised as time passes.

Chairman: Senator Niall Ó Donnghaile is concurring.

Senator Niall Ó Donnghaile: I am in concert with my colleague.

Chairman: I do not think there are other questions we can ask the officials. Our thanks are due to them for accepting the opportunity to attend on the least prestigious of days, unfortunately. All committees are in competition with other events taking place today. We will have to enter private session briefly at the conclusion of this session. I alert the Deputy and the Senator that we have to be brought through the follow-up on this issue before they pack up. I thank the officials for accepting the invitation to attend.

Mr. Deaglán Ó Briain: Ba mhaith liom buíochas a ghabháil leis an gcoiste as ucht a cuireadh.

The joint committee went into private session at 11.30 a.m. and adjourned at 11.35 a.m. until 9 a.m. on Wednesday, 21 June 2017.