DÁIL ÉIREANN

AN COMHCHOISTE UM DHLÍ AGUS CEART AGUS COMHIONANNAS

JOINT COMMITTEE ON JUSTICE AND EQUALITY

Dé Céadaoin, 3 Aibreán 2019

Wednesday, 3 April 2019

The Joint Committee met at 9 a.m.

MEMBERS PRESENT:

Deputy Jack Chambers,	Senator Martin Conway,
Deputy Clare Daly,	Senator Niall Ó Donnghaile.
Deputy Jim O'Callaghan,	
Deputy Mick Wallace,	

In attendance: Deputy Donnchadh Ó Laoghaire

DEPUTY CAOIMHGHÍN Ó CAOLÁIN IN THE CHAIR.

Business of Joint Committee

Chairman: We shall commence in public session. I remind members to please switch off their mobile phones, as they interfere with the recording equipment. Apologies have been received from Senator Black.

We shall first go into private session to deal with housekeeping matters.

The joint committee went into private session at 9.05 a.m. and resumed in public session at 9.30 a.m.

Implementation of the General Data Protection Regulation: Data Protection Commission

Chairman: The purpose of this engagement is to discuss with the Data Protection Commission, DPC, its role following the introduction last year of the general data protection regulation, GDPR, and data protection issues in general. We are joined by Ms Anna Morgan, deputy commissioner; Ms Jennifer O'Sullivan, deputy commissioner; and Mr. Cathal Ryan, assistant commissioner, all of whom are very welcome. We thank them for taking up the invitation to address this very important matter with us.

Before we continue, I must draw the attention of our guests to the situation in respect of privilege. Witnesses are protected by absolute privilege in respect of the evidence they are to give to the joint committee. If, however, they are directed by it to cease giving evidence on a particular matter and continue to do so, 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 are asked to respect the parliamentary practice to the effect that, where possible, they should not criticise or make charges against any person or an 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. Before I call on Ms Morgan to make her opening statement, I again ask everybody, including our visitors, to switch off their mobile phones as they interfere with the recording equipment.

Ms Anna Morgan: We thank the Joint Committee on Justice and Equality for the invitation to attend in order to discuss the recent annual report of the DPC for the period from 25 May to 31 December 2018. I am one of five deputy commissioners at the DPC and head of legal affairs. Accompanying me are Jennifer O'Sullivan, deputy commissioner, who is head of strategy, operations and international affairs, and Cathal Ryan, assistant commissioner, who has responsibility for the consultation function in respect of the public sector and law enforcement matters.

As members will be aware, 2018 was a momentous year for data protection in Ireland and across the EU, with the GDPR entering into application on 25 May 2018. This new legal framework has brought about transformative changes to the data protection regulation system, enhancing the data protection rights of individuals, cementing the responsibilities of organisations when processing personal data, and providing data protection regulators with a new toolbox of hard-edged enforcement mechanisms. While the GDPR is an EU regulation, it allows member states to give further effect to certain aspects of its rules at national level. This was done in

Ireland by way of the Data Protection Act 2018 in respect of which this committee carried out pre-legislative scrutiny in mid-2017. The DPC acknowledges the valuable work carried out in relation to the general scheme of the Data Protection Bill 2017 and the comprehensive report which was produced by this committee as the outcome of that process.

The Data Protection Act 2018 forms a vital piece of the Irish data protection regulatory framework. In essence, the 2018 Act serves three overarching purposes. First, it gives effect at a national level to the GDPR in respect of those areas where a margin of manoeuvre was allowed for member states to specify the GDPR's rules, such as the area of the age of digital consent. Second, the 2018 Act transposed the law enforcement directive into Irish law. That directive provides a separate set of data protection rules relating to the processing of personal data by law enforcement agencies for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Third, the 2018 Act ended the existence of the Data Protection Commissioner and replaced it with the DPC, which is a body consisting of at least one and not more than three people, each of whom is a commissioner for data protection.

Together, the GDPR and the 2018 Act provide the DPC with a greatly strengthened suite of investigative, authorisation and enforcement powers. Under the previous legislative framework of the Data Protection Acts 1988 and 2003, the enforcement powers available to address contraventions of the law were essentially limited to the issuing of enforcement notices. However, under the new regulatory regime, the DPC may issue reprimands and warnings, and impose administrative fines up to a maximum of the higher of €20 million or 4% of annual global turnover. The DPC also has the power to issue directions to organisations to comply with requests by data subjects to exercise their rights, to bring processing into compliance with the law and to issue bans on processing or data transfers, amongst other powers.

The DPC's enhanced medley of powers is reflective of its much increased range of statutory functions under the GDPR and the 2018 Act. These include raising awareness of rights and risks for individuals and of obligations on organisations which process personal data, advising the legislative function of Government on certain legislation, and co-operating with other data protection supervisory authorities in the EU to ensure the consistent application of the GDPR. At the core of the DPC's obligations as the regulator and enforcer of data protection law is the obligation to handle every complaint relating to data protection which is lodged with the DPC and to investigate such complaints to the extent appropriate. In this regard, a significant change from the previous legislative regime is that the DPC is no longer obligated to issue a statutory decision on every complaint where it has not been possible to reach an amicable resolution between the complainant and the organisation concerned. While the DPC must now handle the complaint, it may address the complaint through a number of different actions including, among other things, issuing enforcement notices to the organisation concerned requiring it to take a particular action, issuing advice to the individual concerned, brokering an amicable resolution, or, where appropriate, commencing a statutory inquiry. The DPC has already found that the flexibility offered by the new national legislative regime in this regard has allowed it to make much more efficient use of its resources in seeking to vindicate the rights of individuals rather than having to dedicate significant resources to drafting and issuing statutory decisions. This efficiency is particularly significant in the context of the increased volumes of complaints that are now being received by the DPC, compared with the pre-GDPR period, which I will discuss in a few moments.

It should be noted that while the GDPR and the 2018 Act have been applicable since 25

May 2018, the new legislative regime does not apply retrospectively. Rather, the previous legislation, the Data Protection Acts 1988 and 2003, has been retained in law for certain limited purposes, including for dealing with complaints which relate to data processing prior to 25 May 2018 and for investigations which had already been commenced before that date. The DPC continues to deal with a number of complaints and issues which must be resolved under the previous legislative regime, including complaints which continue to be received in respect of the pre-GDPR period.

The DPC's remit as a regulator is somewhat exceptional in that it applies regardless of industry and sector where any organisation, public or private, with the sole exception of the courts, is processing personal data. However, despite our broad jurisdiction to supervise the processing of personal data, it is important to point out that we do not have regulatory competence in law for many contemporary issues, such as so-called fake news, online content moderation and Internet safety.

Since the introduction of the GDPR, data protection has undergone what the Commissioner referred to in the 2018 annual report as the "GDPR effect"; in other words, the mobilisation of individuals to action to tackle what they see as misuse or failure to adequately account for and explain what is being done with their data. This has been reflected in the significant increase in complaints and queries received by the DPC during the period from 25 May to 31 December 2018, with more complaints received in that seven-month period than in the full year of 2017. Equally, this period has seen a doubling in the number of data breach notifications received by the DPC with the now mandatory requirement on organisations to report data breaches to the DPC within 72 hours. In light of the requirement on the Government to consult the DPC on certain new legislation which concerns data processing activities, there has also been a very significant increase in the DPC's workload to review and provide observations on new and draft legislation, with 25 items of primary or secondary legislation coming to the DPC for review during this seven-month period. Critically, the DPC commenced a considerable number of statutory inquiries under the GDPR during 2018 concerning systemic issues in the commercial and public sectors. Of these, 15 relate to the multinational technology sector, examining issues involving processing by Internet platforms, such as the right of individuals to access their personal data, transparency, the legal basis for processing and the security and safeguarding of users' personal data. A further 33 domestic statutory inquiries were also commenced during 2018, examining issues such as the use of CCTV by local authorities, data breaches by Tusla, and the role of the data protection officer in the Department of Employment Affairs and Social Protection. Each of these inquiries is complex, challenging and raises multiple data protection and legal issues, and the DPC has allocated considerable resources to investigating these issues of systemic public importance. It is expected that the majority of these inquiries will be concluded during 2019. During the period in question, the DPC also took successful prosecutions against five organisations for 30 offences in total related to direct marketing under the regulations known as the e-privacy regulations.

As committee members are aware, the DPC's functions and responsibilities are not solely reserved to domestic regulation of data protection. Under the GDPR and the new one stop shop regime, the DPC has the role of the lead supervisory authority for multinational organisations that have their EU headquarters in Ireland and meet objective criteria to demonstrate that this is their main establishment in the EU. This means that, in addition to handling and investigating complaints from data subjects in Ireland related to these organisations, the DPC must also do so for data subjects in other European Economic Area, EEA, jurisdictions, including when the complaints were originally lodged with other data protection authorities. The DPC is respon-

sible for co-ordinating a consensus on a complaint or a possible infringement of the GDPR with all of the other EEA data protection authorities that are said to be concerned by the issues in question under the co-operation and consistency mechanism of the GDPR.

The DPC's activities in its role as lead supervisory authority represent a considerable proportion of its workload in co-operating with other relevant data protection authorities and keeping them up to date on ongoing investigations and complaint handling. In addition, as a member of the newly established European Data Protection Board, EDPB, which comprises all the EEA data protection authorities, the DPC devotes significant resources to travelling to the monthly EDPB plenary meetings and frequent meetings of its 12 subgroups, with upwards of 100 meetings planned for 2019, all with the aim of ensuring the consistent application of the GDPR.

The very serious expansion of the DPC's remit at national and EU level and the huge increase in workload volumes came as no surprise to the DPC. In the year leading up to the application of the GDPR, the DPC carried out an extensive evaluation and change management process to map the operational and resource impacts of the new functions that the DPC was to take on and the anticipated increases in volume. The Government's increased funding for the DPC during 2018 of €11.7 million, of which €7.3 million represented pay allocation, enabled the DPC to respond to its need for greatly elevated staffing levels and recruit 25 people during the course of 2018, bringing staff numbers to 110. The DPC targeted specialist recruitment during this period, running five specialist competitions with the support of the Public Appointments Service, enabling it to appoint new staff in the legal, investigations and technology areas among others. These appointments were critical for the DPC to continue to build a highly skilled workforce to deliver its expanded regulatory remit under the GDPR. The DPC has continued to increase its staffing levels in the early part of 2019 and the staff head count currently stands at 135, with further recruitment this year expected to take the DPC to 160 staff by the end of 2019.

Strategically, the DPC continued to prioritise its awareness raising activities during 2018, with an ambitious outreach programme of participation in national and international events as well as issuing public information and guidance, undertaking significant media engagement and launching a new website. In conjunction with these ongoing activities, the DPC launched a high profile public consultation at the end of 2018 on the processing of children's data and the rights of children as data subjects. This is with a view to producing guidance materials for children and young people and the organisations that process their data, and encouraging industry to draw up codes of conduct to promote best practices in this area. A further stream of this consultation launched in early 2019, which aims to directly gather the views of children and young people in the classroom through the delivery of a specially created lesson plan. Both streams of the DPC's consultation are running, with a closing date of Friday, 12 April. At a broader organisational level, the DPC commenced a significant project in late 2018 to develop a new five year regulatory strategy, which will include extensive external consultation during 2019. This new regulatory strategy will guide the DPC in prioritising its work and strategically balancing competing demands in the exercise of its regulatory powers, and will give greater insight to stakeholders on how the DPC intends to regulate.

As was 2018, 2019 will be a big year for the DPC, with these consultation projects, its continued expansion and operational enhancement plans and, particularly, with the first wave of decisions arising from its ongoing statutory inquiries anticipated in the latter half of the year. The DPC is committed to firm and robust regulation and looks forward to continuing to break new ground during 2019 under the GDPR and 2018 Act. We thank committee members for their attention and are happy to take questions.

Chairman: I thank Ms Morgan. Almost all of the committee members have indicated and Senator Martin Conway leads the pack.

Senator Martin Conway: I welcome the witnesses. I will ask a couple of questions based on my experience of the GDPR as a public representative. I am sure our visitors are aware that at the very end of the GDPR legislative process a number of amendments were made in the Seanad by the Government with regard to public representatives and Members of the Oireachtas dealing with statutory bodies. I believe many organisations do not respect these amendments. As an example, if my office receives a query about a third level grant and we engage with SUSI, the organisation that deals with third level grant applications on behalf of the Government, the person making the query must go on the SUSI website and name me as an advocate. In my view, this is a clear breach of the GDPR legislation. Have the witnesses come across this situation? Has the commission ever launched an investigation into Departments using the GDPR as an excuse with regard to engaging with people? Has an investigation ever been carried out on organisations that perhaps implement the GDPR legislation in a way that is not appropriate? Has the commission policed or looked at any examples of where the amendments made to the legislation regarding how public representatives engage with various Departments are implemented at local authority level or Department level?

Chairman: Who would like to take up this question? Does Ms Morgan want to answer? All of the witnesses should feel fully at their ease to add something and they should indicate.

Ms Anna Morgan: I thank the Senator for the questions. I will deal with the latter issue he raised in general terms and then hand over to Mr. Ryan on the specific query raised. The Senator referenced the phenomenon of the GDPR being used potentially as an excuse to deal with certain issues. This is certainly something the DPC has been aware of in many contexts since the GDPR came into application. The rules in the GDPR have been used by a range of sectors potentially to sidestep obligations that may otherwise apply to them. We have had to do a significant amount of myth busting. Recently, we published a blog on our website on what the GDPR does and does not state. The issues raised by the Senator are certainly very pertinent in the context of the first ten months of application of the GDPR.

On the substance of the question, which I understand concerns section 40 of the 2018 Act and the activities of elected public representatives, I will hand over to Mr. Ryan to address it in more detail.

Mr. Cathal Ryan: We identified the issue as important very early. Literally post-GDPR we noted that there were issues in terms of making public representation. It is important to state that it is a really important democratic function. We were very aware that we needed to discuss this matter not only with Members of the Houses of the Oireachtas but also with local authorities and the Departments, which is what we did. Behind the scenes I carried out a lot of consultation with various committees and local authorities through the Local Government Management Agency, LGMA, to get a sense of the issues on the ground. Following that, we identified that there was an inconsistent approach being used either by local authorities or Departments in how they approached section 40 of the Act. With that in mind, as the Senator rightly pointed out, there is a sense that people or the Department were using GDPR as an excuse. We wanted to tackle and implement a common sense approach to section 40, which we have done through the publication of guidelines. The guidelines would have been sent to every Member of the Houses of the Oireachtas. Those guidelines were also issued to all local authority and public sector departments nationwide. The guidelines suggest that a democratic representative must take some responsibility for the public representation that he or she is making in terms of en-

gagement with his or her constituent. On the basis that they have done so, the Department or a public sector body should take his or her word or a written letter that he or she has a legitimate public representation to make. If one reads the guidelines, which were published late last year and, I believe, around December, one will get a real sense of what is required. Following the guidelines, which we published, we then went back to those bodies and encouraged them to come together and form a standard approach. For example, I have attended a data protection officer, DPO, network committee with the LGMA for local authorities and I understand that they will develop a code of conduct based on these guidelines. As Members will be a aware, there are 31 local authorities that may be doing 31 different ways of public representation.

Senator Martin Conway: I do not believe that the guidelines are good enough or respect the spirit of section 40 of the GDPR legislation that we put through the Houses of the Oireachtas. The guidelines do not respect the unique electoral situation that we find ourselves in. There are only two countries in the world that have a similar electoral PR-STV system - Ireland and Malta.

The amendments were brought in, in the Seanad, to deal with the uniqueness of our political system. Yesterday, I spoke to the staff in my office and asked them for one example, which was SUSI. Do the witnesses think it is acceptable that a Member of the Oireachtas should have to ask a client to go on the SUSI website and name him or her as an advocate given the fact that we have an applicant's personal public service, PPS, number, date of birth, address and all other relevant references? Do the witnesses think it is acceptable that a Member of the Oireachtas should have to demean him or herself and ask a client to go on a website of a public body to name him or her as an advocate?

Mr. Cathal Ryan: No, is my answer. When one reads and assesses the guidelines one will find that they suggest a common sense approach. It appears to be that an overly bureaucratic approach is being taken in terms of what SUSI is doing. We must be mindful, as a regulator, that the principle of accountability means that each data controller must make an assessment of how they will approach public representation. Our guidelines were there to influence how the assessment is made. The guidelines are being digested at the moment because they were issued in December of last year. Once public sector bodies and local authorities have considered the guidelines we are then going to follow up by encouraging a standard approach but a less bureaucratic common sense approach. We cannot get into every detail of what they will do in terms of safeguarding particularly sensitive data. One thing we can do in terms of the SUSI application that was mentioned-----

Senator Martin Conway: I gave just one example.

Mr. Cathal Ryan: Yes, but it is a common sense one. When one writes to SUSI then that should be the public representation verified without an individual having to fill in a form, which is five or six pages long. Sometimes doing so delays the process. I mean the objective of the public representation cannot happen because of a delay in bureaucracy and filling out forms. We have asked and encouraged bodies to read our form and guidance but apply it accordingly. We anticipate that the guidelines will work. Obviously there will be individual things that will happen, o a case by case basis, that we will have to consider. In the main it is expected that public sector authorities will apply a common sense approach to this very important function. If there are issues with the interpretation of our guidelines or an overly conservative approach being taken by a public sector authority then of course we will consider the matter. One must bear in mind that we cannot compel a body to share information and it is their assessment based on the principle of accountability.

Senator Martin Conway: I challenge Mr. Ryan's claim that his office cannot compel. If a Member of the Oireachtas breached data protection then his office would be able to carry out an investigation. There is no point in us dominating this discussion. I would say that his office has a duty of care and responsibility to host a workshop here and engage with Members of the Oireachtas. We can give practical examples of where our work has been impeded by Departments using the GDPR as an excuse. Perhaps Mr. Ryan and his senior management team can discuss the matter and come back to us with a plan.

Mr. Cathal Ryan: Yes, Senator. We had an open invitation to do just that. Following the release of guidelines we communicated that offer to the Houses of the Oireachtas. We have done it in terms of recently meeting councillors at an annual conference by the Association of Irish Local Government, AILG, in Longford. I am sure the members are familiar with the association. We have carried out conferences and workshops of this nature. We are very much open to continuing that work and spreading the message that people should adopt a common sense approach to public representation.

Chairman: Before Senator Conway leaves I must emphasise that he used the word "impeded" and, as Chair of this committee, I want to say to the witnesses that it is not just an isolated individual experience. I am saying, in full support of what Senator Conway has said, that this is a universal experience and impeded is exactly what is happening in terms of our representative function. It is a very serious matter and I cannot underscore it strongly enough for the delegation here this morning and thank the Senator for his contribution.

Senator Martin Conway: If this engagement achieves nothing else but respect for the fact that people who are elected to public office have a mandate, and the confidence and support of the public who elect them, it will be a good thing. Let me outline why section 40 was brought in. I lobbied significantly for the section. When one peruses the record of the House one will see the engagements and contributions on both Committee and Report Stages. The work was done because we are in a situation in this country where politicians receive thousands of representations on specific issues whether it is social welfare, health, education and so on and I really do believe that the commission has a job of work to do. If this engagement achieves nothing else but re-establishes respect for public representatives among public bodies then it will be a good engagement.

Chairman: I thank the Senator and call Deputy Jack Chambers.

Deputy Jack Chambers: I thank the witnesses for being here. Like Senator Conway said, perhaps the commission would provide a specific email or phone line that would allow public representatives to submit something that restricted our ability to do our representative function. If that were communicated to us, it would be a helpful way for the commission to go directly to whomever the body is or the person who is going beyond what the GDPR provides. I have some questions on the commission's relationship with the various technology companies. What engagement has the commission had with them? What is the level of co-operation it has had? Does the commission give them notice if it is conducting an audit or does it conduct randomised audits of their data processing? What is the relationship with them on a day-to-day basis?

Ms Anna Morgan: In general terms, as members may know, the DPC has always reinforced the importance of an ongoing dialogue with multinational and technology companies to drive better awareness and increased understanding of the rules on data protection and, in particular, the interpretation and position of the GDPR in respect of those rules. The ongoing dialogue we have with companies serves a very important function and has resulted in us be-

coming aware of the potential roll-out of products and services where we can input into the data protection compliance of those products and services and influence the technology companies on the manner in which they intend to move forward where we perceive risks to data subjects.

The statutory inquiries we have opened involve a completely different process to our consultation and engagement function. Those statutory inquiries, 15 of which were opened into the multinational sector during 2018, have as their ultimate objective the reaching of a decision on whether there has been an infringement of one or more of the GDPR rules. There are a number of stages to those processes and they are quite formalised. Our annual report refers to the overall linear process. Members will see a graphical depiction of that on page 30 of our annual report. In essence, the process involves the stages of information gathering, evidence collection, setting the scope of the inquiry and applying the law to the evidence gathered to assess whether there appears to be an infringement of the legislation. There is then the formal decision-making process whereby the decision-making function in the commission is engaged to make a formal decision which has status under the 2018 Act and to then consider whether, if an infringement has occurred, a corrective power should be applied. That is a very different process from the supervision function. I might hand over to my colleague, Ms Jennifer O'Sullivan, to say a bit more on the supervision of multinational companies and, in particular, statutory inquiries.

Ms Jennifer O'Sullivan: As Ms Morgan said, we opened 15 inquiries in total during the period covered by our recent annual report into those large multinational technology companies. The inquiries cover a range of fundamental data protection matters. Fundamental transparency obligations are being examined and fundamental elements of data protection law as to the legal basis for processing are being carefully looked at. In light of the breaches reported by two of those companies during that period, we have examined the organisational and security measures of a couple of the companies under the format of a statutory inquiry. Regarding the relationship with the organisations, we have a multifaceted approach. Some of our engagement with them is in the context of consultation around their new products. It is also important for us is to get a better understanding of their business models and the context in which they work. That is important and useful for us as regulators with regard to the efficacy of our advice as well as with regard to our decision-making and judgment in separate contexts. Those are some of the inquiries we have under way. Since the start of 2019, we have commenced to open further inquiries.

Deputy Jack Chambers: Of the 15 complaints, seven are against Facebook and two are against WhatsApp, which is a company under the ownership and jurisdiction of Facebook. As such, that is nine out of 15. When will fines issue or decisions be made? In France, decisions have been made under EU privacy rules and a fine has been issued to Google of €50 million. Google has its headquarters here. When will decisions and outcomes emerge under the GDPR investigations? People are awaiting that. What is the timeline or trajectory for the decision-making process to conclude?

Ms Jennifer O'Sullivan: The Deputy is right that we have seven inquiries into Facebook, two into WhatsApp and a further inquiry into Instagram, which is also owned by Facebook. That represents a significant proportion of our formal inquiries. Some of the inquires were in response to complaints, as the Deputy said, but others we undertook of our own volition having examined the context and wider situation. On the timeline, my colleague outlined the very structured, formal, robust and consistent approach we need to take to these inquiries. The latter elements of the process include engagement with our colleagues around the EU in the format of the European Data Protection Board. We are obliged to consult with those colleagues as we

near the decision-making process. We must submit a draft decision to those colleagues which they are entitled to examine and submit reasoned and relevant objections on. We must take account of those objections, consider whether they have a bearing on our draft decision and seek consensus. That process takes time in its own right.

The decision of our French colleagues on the Google case involved a somewhat different situation. Google only established itself as a controller in Ireland in January 2019. Prior to 22 January 2019, any data protection authority around Europe with competence could have examined a complaint brought to it and taken enforcement action. That is what our colleagues in the French data protection authority, the CNIL, did. A complaint was submitted to them at the end of May and at the time the GDPR came into effect. The CNIL engaged in collaboration and discussion with ourselves and other members of the European Data Protection Board to ensure we carefully examined the question of competence given that Google had not established a data controllership in the EU at all. After that careful examination, we concluded that it was a matter for the CNIL to take up directly. However, because it did not come under that definition of cases that are examined under the one-stop-shop model, the CNIL did not have to go through those stages of consultation with colleagues around the EU and EEA on the case. It was a much shorter process which is why it was able to announce its decision on 21 January this year. With the inquiries under way here, we are facing into that consultation process with those colleagues.

Deputy Jack Chambers: Paragraph 7 of the opening statement referred to changes to the data protection legal framework and pointed out that the DPC has no regulatory competence in law for many contemporary issues, including fake news, online context moderation and Internet safety. Has the commission a view on a digital safety commissioner and on the debate on fake news? Has it examined what has happened elsewhere?

Ms Anna Morgan: On a digital safety commissioner, we have noted that a public consultation process has been launched by the Government and is ongoing. The consultation concerns the bringing into effect of legislation on online safety. The legislation is also intended to transpose the EU's audiovisual media services directive. Insofar as there is an intersection between data protection and issues of online safety, it occurs in relation to children in particular. Data protection authorities have a newly enunciated obligation under article 57 of the GDPR to drive awareness of issues relating to children's rights and the risks for them in the processing of their data by organisations. We have been exploring this issue during the course of 2018 to try to identify methods by which we could better raise awareness and drive good practices among organisations, particularly in the online sector. With a view to doing that, as I referred to in my opening statement, we launched a consultation process at the end of 2018 which has two limbs to it. The first is a written public consultation aimed at adult stakeholders. Parents, educators, child protection organisations and children's representative groups are all encouraged to take part in this consultation, which engages a range of issues from transparency information to children to enable them to understand what is happening to their data when they engage in the context of online platforms and apps. It also covers issues such as the appropriate age at which a child should be able to exercise his or her data protection rights because the GDPR is silent on that issue. However we are conscious of the UN Convention on the Rights of the Child and the particular provisions that relate to children having a right to have a say, in light of their evolving capacities, on matters that directly concern them.

The consultation also relates to issues around direct marketing and advertising to children and the use of children's data in that context. Along with topical issues, of which the committee members will be aware, it relates to Article 8 of the GDPR concerning the age of digi-

tal consent and issues around age verification, including the verification obligations on online organisations to establish that consent to processing has been given by the holder of parental authority. In light of all of these issues, which have been to the fore of public discussion in the past two years, we launched this consultation process. We were also very keen to engage with children directly. For this reason, we made the unique decision to launch a further stream of our consultation, this one aimed at garnering the views of children in particular. We explored different methods by which we could more effectively do that and we decided that participation in a standard written consultation was potentially not the most effective way to gather children's views. For this reason, in 2018 we designed a series of lessons plans from scratch, which aims to educate children in a classroom setting on basic principles of data protection to make them aware of their rights and the risks when they are sharing information in an online setting. These education materials have been sent to every school and all of the Youthreach centres.

The timeframe for the consultation is still ongoing. We have asked teachers in schools to participate, obviously on a voluntary basis, in delivering those lesson plans. The ultimate output of those lesson plans is an exercise whereby teachers can gather the views of children on the topics that have been discussed. They can also share their opinions on issues such as the age at which children should be able to make an access request to an organisation or seek the erasure of data they have shared online. That consultation is ongoing and at the end of the process, the intention is to produce best practice guidance for organisations on the use of children's data and, importantly, guidance for children which will be written in accessible and easy to understand language to help them to better comprehend the issues around sharing information online. Connected to that and in light of our obligation, as set out in the 2018 Act, to encourage the drawing up of codes of practice by industry on a range of issues concerning the processing of children's data, we also aim to use the outputs of that consultation to encourage industry members to come together and produce those codes of conduct.

Deputy Jack Chambers: How is the digital age of consent being implemented? Have many complaints been made about breaches of the legislation? Has there been any investigation into breaches of the legislation?

Are the resources allocated to the Data Protection Commission commensurate with the commission's role in the context of multinational companies? The Data Protection Commissioner, Ms Dixon, has outlined publicly her concerns about the general allocation, staff space and other matters. Will Ms Morgan update the committee on those issues?

The Minister of State at the Department of Justice and Equality, Deputy Stanton, will be before the committee to discuss gambling companies next week. There are a great many concerns about gambling addicts, one of the most vulnerable groups cohorts in society, being targeted on the basis of their previous activity. The gambling companies use very complex technical tools to target people and there may have been data breaches. Concerns about this have been submitted to the Data Protection Commission. Are there active investigations under way against gambling companies?

Ms Anna Morgan: I thank Deputy Jack Chambers for his questions. On the age of digital consent, which relates to Article 8 of the GDPR, which is a challenge in itself in regard to the obligation on organisations to take reasonable steps to verify that consent has been provided by the holder of parental responsibility where consent is the basis for processing children's data, in other words, the data of anybody in Ireland under the age of 16 years. This goes to one of the core issues we are considering in our consultation, namely, how organisations can adequately verify age to identify whether a child falls below or above that threshold. Connected to that,

there is the obligation on organisations and online platforms to verify parental consent in regard to that processing. A range of different methods has been used by organisations, some of which have been based on the Children's Online Privacy Protection Act 1998 in the US, known as the COPPA Act. COPPA is detailed legislation that specifically deals with these issues and sets out a range of different techniques, whereby organisations can potentially attempt to verify that the holder of parental responsibility has given consent to the processing. One of the methods referred to in the legislation is the use of micro-payments on a credit card, the theory being that somebody over the age of 18 years will have access to a credit card. We are aware that certain online organisations and companies rolled out this measure as a means of verifying whether consent had been adequately given. We are aware that those companies have received a certain amount of criticism from parents who believed that the gathering of this additional financial information was excessive and disproportionate to the obligation on the organisation to verify parental consent. It is a very complex issue and one that we intend to fully explore in the context of our consultation. We will address it in the best practice guidance that we intend to issue after the closure of that consultation.

On the issue of the allocation of resources and staffing levels for the organisation, the Data Protection Commissioner has mentioned on a number of occasions that from 2014 onwards, the Government committed to increasing the funding of the Data Protection Commission in that year and to keeping it under review. It has done this and the budget allocation to the commission has increased every year since 2014. The budget for 2019 is €15.2 million, which is a dramatic increase from the €1.7 million allocated for 2013. We are very much of the view that adequate funding for the Data Protection Commission is critical for it to continue to build its capacity and enable it to perform as an internationally respected, effective and robust regulator. We have very much welcomed the increases in the budget in recent years.

In terms of the impact of the budget on staff, as I mentioned in my opening statement, we currently have 135 staff and we intend to recruit further staff in specialist areas by the end of this year, particularly in the legal, technology and investigatory functions. These are priority areas of recruitment for us. We intend to reach a staff complement of 165 by the end of 2019 based on this year's current budget allocation. We also anticipate that we would need 190 staff by the end of 2020 and 220 staff by the end of 2021, based on our analysis to date of the trends and increasing volumes of matters that we are dealing with. The funding issue remains vital to us being able to continue to perform in the manner that we must do, under the GDPR, and fully perform our functions under the expanded remit of the new legislation.

Finally, I shall deal with the question on gambling. We do not have a regulatory remit for the gambling sector *per se*. However, there will be or may be many situations where personal data could be used in the context of the gambling sector. Some of the issues referred to might relate to online behavioural advertising, which is an issue that the office has examined in a number of different contexts. My colleague, Ms O'Sullivan, will comment on the issue of online behavioural advertisements.

Ms Jennifer O'Sullivan: I thank Deputy Chambers for his question. The office is examining the issue using a multi-pronged approach. At European level we are working with our colleagues in the European Data Protection Board as part of a subgroup that examines social media and the targeting of individuals through social media. We are working on the issue in a very universal way, which would include the targeting of vulnerable individuals such as gambling addicts that were mentioned by the Deputy. The Data Protection Commission is comprehensively examining the issue. During 2018, we established a technology leadership unit, which

is doing significant research into the area of advertising technology or adtech that touches on some of the issues that have been mentioned. We are also examining complaints and submissions from various groups who are concerned about the area and we are very carefully examining our statutory steps on that.

Chairman: I thank the Deputy and the representatives of the commission. I call Deputy Wallace.

Deputy Mick Wallace: Deputy O'Callaghan has two questions and wants to leave so I suggest we allow him to contribute now.

Deputy Jim O'Callaghan: Is that okay, Chairman?

Chairman: There will be a reshuffle, by agreement.

Deputy Jim O'Callaghan: I thank the witnesses for coming in. I want to ask them about the investigations the commission can conduct under sections 137 and 138 of the Act. Has the power in section 137 that requires people to attend before the authorised officer been invoked?

Ms Anna Morgan: A section 137 investigation is a step that can be taken in the context of a statutory inquiry that is commenced under section 110. Section 137 represents a particular set of powers that can be invoked by authorised officers, in particular, an authorised officer once section 137 is triggered in the context of an ongoing statutory inquiry. The authorised officer can, for example, hold an oral hearing and has more extensive powers than the standard powers of authorised officers, under section 130, to compel evidence on oath and a range of other particular powers. That power has not been activated to date but we keep the exercise of our powers under review. Each inquiry will depend on the context, the level of co-operation by the organisation in question, and the manner in which we need to go about gathering evidence and collating information on the scope of the particular inquiry. The question of what powers are exercised at what point will really be very much context dependent.

Deputy Jim O'Callaghan: Has the power to require somebody to attend before the commission or conduct an oral inquiry been invoked?

Ms Anna Morgan: Neither of those powers has been invoked to date.

Deputy Jim O'Callaghan: The role of an authorised officer is performed by somebody from within the DPC. Is that correct?

Ms Anna Morgan: That is right at the current point in time in the context of all of the 49 inquiries that we currently have open. However, the legislative provisions for the authorised officer make it clear that there is scope for persons other than staff of the commission, depending on whether they are deemed to be suitably qualified, to be authorised as authorised officers. In the context of the GDPR and the provision for co-operation in particular joint operations, which can be carried out between European data protection authorities, potentially, the provisions in the 2018 Act will allow for the authorisation of officers from other European data protection agencies to take part in our investigations.

Deputy Jim O'Callaghan: Under what statutory provision are the 17 investigations into the big tech companies taking place?

Ms Anna Morgan: They have all been commenced under section 110.

Deputy Jim O'Callaghan: What needs to be done to transpose cases into a section 137 investigation?

Ms Anna Morgan: Section 110 refers to the overall framework for a statutory inquiry. A section 137 investigation is a particular step.

Deputy Jim O'Callaghan: Has that step been taken as of yet in any of the investigations?

Ms Anna Morgan: No, it has not been taken. It very much depends on whether we need to exercise the additional powers that section 137 allows for.

Deputy Jim O'Callaghan: I thank Ms Morgan.

Deputy Mick Wallace: I thank the witnesses for coming in. My apologies but I am a bit hoarse. We have talked about this stuff for nearly two years but it seems like a lifetime and yet I still do not understand it all. I do not envy the delegation their jobs. I would rather be pouring concrete in my bare feet than do their job. I have prepared a number of questions, which are a criticism and simply seek more information. A lot of it springs from our encounters with the Ministers while we debated this stuff over the period. I have broken my questions into a couple of different sections.

As much as 30% of all complaints from 25 May to 31 December 2018 and 39% of all complaints made in the same period. under the pre-GDPR Acts, were access rights complaints. In terms of the number of complaints received, access rights complaints were the biggest issue. Does the delegation have a breakdown of the different types of access rights complaints? How many relate to the one-month time limit for organisations to comply with access requests? Are statistics available on the length of time that elapses between receiving a complaint, initiating an investigation and completing an investigation? Howe does the DPC enforce the one-month limit for organisations to comply with access requests? What enforcement options are available if an access request complaint cannot be resolved amicably as with case study No. 5 in the report?

I appreciate that the DPC is the *de facto* European regulator and has an enormous amount of work to get through. According to anecdotal evidence provided to me by various people who have made access rights complaints to the DPC that it is slow to deal with a complaint that a data controller has simply ignored an access request. If these procedures and delays are a result of insufficient funding then the funding of the DPC should be examined. If the cause is something else then perhaps the way the complaints are handled needs to be examined. Ms Morgan said that the DPC has 135 staff at present, and that there will be 160 staff by the end of the year and 190 staff by the end of next year. Is that enough staff?

Ms Anna Morgan: I ask my colleague, Ms O'Sullivan, to address the first set of questions.

Ms Jennifer O'Sullivan: In terms of access requests and the complaints we receive about them, a significant proportion relate to the one-month deadline being missed and a further significant proportion would be on the completeness of the information provided. We can give the Deputy a breakdown of the figures.

In terms of the length of time between the DPC receiving a complaint and initiating activity, the Deputy is right that speed partly depends on the level of resources that we can apply. As resources are increased the time shortens. We are tracking that performance measure very carefully and seeing a slight reduction in it.

Further to the question asked by Deputy Jack Chambers, and the response given by my colleague, Ms Morgan, the question of funding and resources relates to the level at which we can simultaneously handle complaints and enforce. Certain finite parts of each process need to be run through. Certainly, we could do more simultaneously if we had more resources. The Deputy's question related specifically to the length of time that passes between the receipt of a complaint and the initiation of an investigation. When we receive a query, concern or complaint from an individual, we check if the issue relates to data protection to ascertain whether it is within our competence. After that has been assessed, generally we seek initially to resolve the matter amicably between the individual and the organisation. Access requests, in particular, tend to turn on their own facts. By intervening and engaging with the data controller and the individual, we can quickly achieve a vindication of the individual's rights and ensure that through our intervention, he or she receives the full set of data he or she is seeking from the data controller. It is not the case that each complaint ultimately ends up as an investigation. That is particularly true in the case of access requests if it seems like the issue is specific to the case. A small proportion would reach a statutory basis like that. Ms Morgan might follow up on this. When we achieve amicable resolution of a specific case, we always examine the issue in general with the data controller. The achievement of an amicable resolution in a given case does not preclude us from continuing to examine the issue in a more systemic way. Ms Morgan has more to say about amicable resolution in general.

Ms Anna Morgan: It has been outlined in a number of case studies in our annual report that amicable resolution is a valuable method for achieving the vindication of the rights of data subjects. In our experience, most of those who make complaints to our office are satisfied when they achieve the vindication of whatever right they had been trying without success to exercise against the data controller; for example, when they have received the information they sought in an access request or achieved the erasure of information. Generally, it is not necessary to take further enforcement steps. A question was asked about the enforcement methods that are available when we are unable to reach an amicable resolution because the data controller is not inclined to allow the data subject to exercise his or her rights. Sometimes the complainant is not prepared to accept an amicable resolution. That may relate to the general backdrop to the complaint. We often find that data protection is the prism through which many consumer issues come to the fore. For example, overcharging by banks or phone companies can be a frequent occurrence. If there is a more complicated background to the complaint, the complainant might not be prepared to engage in the amicable resolution process. When we encounter difficulties in getting a data controller to comply with a data subject's request, section 109(5) gives us the power to issue enforcement notices to direct the data controller to do a number of things, such as comply with a particular request or notify a data breach to an individual if that has not already been done. More broadly speaking, we have a range of more general enforcement powers where a complaint might turn into a statutory inquiry.

Deputy Mick Wallace: According to page 45 of the annual report, which provides an update on the public services card investigation, a draft report of the investigation containing "13 provisional findings" was issued to the Department of Employment Affairs and Social Protection for comment in August 2018. I am curious about the use of the word "provisional" and I ask our guests to elaborate on it. In what way are the DPC's findings in the draft report provisional or subject to change? While I am familiar with the statutory inquiry workflow as outlined in the annual report, I am curious to know whether the DPC's findings at this draft report stage might change based on steps taken by the Department as the data controller in the period between receiving the draft report and the DPC's final decision, for example to address issues of coerced consent or the lack of a legal basis for processing. Is it the case that the findings are

provisional because the data controller might offer a further defence against the findings contained in the draft report? Perhaps out guests could comment on the concerns that this process involves a certain amount of collaboration between the regulator and the data controller.

The workflow of the statutory inquiry is set out on pages 28 to 30 of the annual report. Is it the case that step 6 in the process, in which the "DPC decision-maker notifies [the] DPC draft decision to other concerned EU data protection authorities", is necessitated by Article 60 of the GDPR, which refers to "Cooperation between the lead supervisory authority and the other supervisory authorities concerned"? Is the statutory inquiry process, including for example the European Data Protection Board dispute resolution phase of the process, the same for all DPC statutory inquiries? Is the same process or workflow for these types of investigations used by all data protection authorities in the EU? Do our guests think this process is applied in a consistent manner across the EU?

Late last year, a spokesperson for the DPC indicated that no more than a summary of the parts of the final public services card report which are deemed to be in the public interest would be published. I ask our guests to elaborate on what is meant by the public interest in this context. How could it be in the public interest to conceal aspects of an investigation? Do our guests agree that if the full report is not published, there will be a problem with the transparency of the investigation? As I see it, this investigation has real potential to be a definitive or landmark statement by the DPC on data processing in the public sector, regardless of how the DPC rules on the various elements of the investigation. During Question Time in the Dáil last month, the Minister, Deputy Regina Doherty, told me she "would have the legs cut off" her if she went against the DPC's clear instruction not to release the draft report. The Minister did not understand my question. I was actually asking about the possibility of publishing the DPC's final decision, rather than the interim or draft report. Will our guests clarify whether the DPC has instructed the Minister not to publish the draft report? If it has, why was such an instruction given?

Ms Anna Morgan: I would like to preface my response to the Deputy's queries about the report that has been produced as part of our ongoing investigation into the public services card by saying there is a limit to how much we can say about an ongoing investigation. Members will be aware of case law in respect of to issues such as prejudgment and the issuing of comments that could potentially raise concerns regarding bias or the predetermination of issues. The investigation is still very much ongoing.

The Deputy referred to "concerns [around] collaboration between the regulator and the data controller", which in this context is the Department. I refute that comment absolutely. There is absolutely no collaboration. As an independent regulator, we have to investigate the facts of the issues that are to be determined in the scope of an inquiry. We do that in an entirely independent and impartial manner. The steps we follow in any investigation must accord with the right of all of the parties to any given process to fair procedures and procedural safeguards. The report in question, which was issued on a provisional basis to the Department, is said to be provisional because it allows for the Department's right to be heard. As the Deputy will be aware, this is a fundamental aspect of natural and constitutional justice within our legal system. Phraseology such as "provisional" is used to denote the fact that submissions were allowed to be received. The Department was given an opportunity to make submissions on the report addressing any aspects of the provisional findings which it did not consider to be an accurate reflection of the factual or legal situations, in order that we could take account of such matters in our further considerations and in finalising the report.

The Deputy also asked about the overall timeline for that report. As referred to in our annual report, we received a significant volume of submissions totalling approximately 470 pages of documents from the Department in response to our invitation to make submissions. We are in the process of reviewing that material.

On the overall scope of the ongoing investigation, this has not been a static inquiry. There has been an element of dynamism as certain things have changed in the course of the investigation. For example, one of the issues that is, of course, being investigated relates to the question of transparency and information that is given to data subjects by the Department. During our investigation, the Department published a comprehensive guide to use of the public services card, PSC. It also published for the first time a consolidation of the relevant social welfare legislation in this area. The scope of the inquiry has had to move to take account of these changes. Additionally, members will be aware that the practice in regard to the use of the public services card to obtain a driver's licence has changed considerably in the course of our investigation. For example, between June 2017 and August 2018, a PSC was required to sit the driver theory test but, as of 20 August last year, the PSC became one of a number of acceptable forms of identity confirmation in that regard. The investigation is somewhat dynamic. We anticipate that it will conclude within the year with the issuing of our final report to the Department.

On the issues raised by the Deputy around publication of the report, the investigation has been conducted under the previous legislation, namely, the Data Protection Acts 1988 and 2003. Our powers of publication are constrained and determined by the extent of the powers set out in those Acts. Although the 2018 Act provides for express powers of publication under section 141, there is no equivalent section in the previous legislation. However, if the Department were to consent to the publication of that report, we would very much be open to considering its publication in full with the caveat that, obviously, consideration would have to be given to any confidential information that was not amenable to publication. Overall, we have no objection to publication of the report once it is finalised.

Deputy Mick Wallace: Will the commission recommend to the Department that it be published?

Ms Anna Morgan: We will certainly draw the attention of the Department to the issue and raise the matters that have been addressed by members during this meeting.

Deputy Mick Wallace: Would the commission consider a company using facial image matching software to match a photograph of a person to other photographs or digital images stored in a database to be processing biometric data? Does this kind of facial image matching meet the definition of biometric data in Article 4(14) of the GDPR and the reference therein to "specific technical processing"? Last year, the Data Protection Commission issued guidelines in respect of biometric data. One type of biometric data it identified was raw images consisting of recognisable data such as an image of a face or a fingerprint. This appears to be in agreement with the Article 29 Working Party example of biometric data which specifically mentions a photograph of a face. It seems obvious to me that a photograph is a raw image consisting of recognisable data such as an image of a face. I ask the witnesses to confirm or clarify the position of the commission on the biometric nature of a photograph? Are photographs biometric data?

Ms Anna Morgan: The issues referred to by the Deputy around the processing of biometric data concern the processing of special categories of personal data under the GDPR. I will hand over to my colleague, Mr. Ryan, to address that issue in more detail.

Mr. Cathal Ryan: Article 9 of the GDPR sets out conditions for processing of special category data. Biometric data is included within that. Under Article 9, it is considered a derogation. Effectively, in order to process sensitive data, one needs to rely on one of the derogations set out in Article 9(2). One will see what measures need to be implemented, such as explicit consent or whether it is in the public interest, which is distinguished to be "for reasons of substantial public interest". The processing of biometric data and, in particular, facial recognition software involves the area covered by Article 9 and one will need to satisfy a condition under Article 9 to proceed. I have not carried out any assessment of the case of which the Deputy may be aware, although I think he is raising it more as a general issue.

Much of this issue comes down to the kind of processing that is taking place. For example, processing sometimes takes place in an airport in a situation where there is no attempt to attach any personal information but, rather, to measure a queue. Is there processing of personal data in measuring a queue of individuals coming into an airport and leaving through the security gates? There are different types of processing taking place. There is an important distinction between matching facial data to other data and just looking at individuals moving through an airport queue but not trying to match that data with anything else. Much of the issue comes down to the processing itself, the nature of the processing and whether there is matching of data with other personal data such as the person's name and so on.

Deputy Mick Wallace: I was glad to see that the section of the annual report dealing with special investigations states that the Data Protection Commission has initiated a section 110 inquiry into surveillance by the State sector for law enforcement purposes. The smart CCTV project of Limerick City and County Council seems to have been abandoned because it will not comply with the GDPR and the Data Protection Act. Approximately €350,000 was spent on the project, which is a crazy waste of money. We previously raised problems with the scheme in the Chamber and warned about the lack of a legal basis for it. It proposed that deep learning and artificial intelligence be overlaid on a network of cameras that could count footfall, keep a record of the registration of every passing car 24 hours a day and recognise faces and patterns. Section 38 of the Garda Síochána Act 2005 specifies that CCTV schemes should only be authorised for securing public order and safety in public places, but the proposals for the project published by Limerick City and County Council stated that the scheme would be used to monitor tourism and, bizarrely enough, for animal control. I hope that the decision of the Data Protection Commission regarding CCTV schemes and law enforcement surveillance will, when published, deter other public bodies from wasting such an amount of money on a mass surveillance project that does not have a legal basis.

Last year, I tabled a parliamentary question to try to establish if there were limits on the technology that could be used as part of the Department of Justice and Equality community-based CCTV scheme. The annual report indicates that the Data Protection Commission is investigating automatic number plate recognition cameras, for example, as part of its inquiry. Section 31(d) of the Garda Síochána (Policing Authority and Miscellaneous Provisions) Act 2015 bestows responsibility to publish guidelines in respect of CCTV cameras on the Policing Authority. I wrote to the Policing Authority in March of last year regarding the use of automated number plate recognition and facial recognition cameras as part of the Department of Justice and Equality community-based CCTV grant aid scheme. The Policing Authority confirmed that, rather strangely, it had not yet issued any guidelines under section 38 of the Act and the Department had not issued guidelines before the Policing Authority was established. As far as I am aware, no guidelines have yet been issued. However, the Policing Authority also stated in its reply to me that it has no role in respect of the technical specifications of CCTV cameras.

Neither the Minister nor the Policing Authority seems to have any responsibility for this issue. I submitted a freedom of information request to the Policing Authority seeking further information on any work it may have done on CCTV guidelines. In a 2017 comparative research paper on CCTV, the Policing Authority suggested that a code of practice might be a better idea than required guidelines. However, that would require section 38 to be amended. The Policing Authority also suggested in papers released under a freedom of information request that drafting a code of practice would really be a job for the Data Protection Commission rather than the Policing Authority. In an email sent in September 2017, the head of legal policy and research at the Policing Authority addresses the statutory role in regard to CCTV. The email states that there is limited value in the Policing Authority putting such guidelines in place and that most of the issues in respect of monitoring of CCTV come under the remit of the Data Protection Commission. Will Mr. Ryan confirm whether the DPC has had any contact with the Policing Authority in respect of these matters and whether it intends to make a decision on the technical specifications of the surveillance equipment it will permit to be used? I refer to how powerful or intrusive such equipment might be.

Mr. Cathal Ryan: The Deputy raised several pertinent issues we are keenly aware of he asked quite a few questions. I hope I can answer all of them but if I do not-----

Deputy Mick Wallace: Mr. Ryan may send me the answers if he does not finish.

Mr. Cathal Ryan: I will provide an outline of what we are doing. The committee will be aware that we have taken it upon ourselves to begin an investigation of community CCTV, the intention behind which is to discover what is happening. As indicated earlier, 31 local authorities operate the scheme, perhaps in a different manner, although a code of practice is in place. This is currently under review and our inquiry will assist in that regard. The inquiry has been outlined and we provided an update on the status in our annual report. It will take time because we must engage with 31 local authorities on the issue. I noted in a report that the work the committee has done this month in respect of rural policing and so on is important. We are cognisant that we need to get the matter right. One of the issues that has arisen is accountability, that is, who is responsible and who is administratively responsible for the data collected. As part of that investigation, other technologies may come to the fore, such as automatic number plate recognition, which the Deputy mentioned. On legislation, we expect the legislative provision to allow for it. In the absence of a specific legislative provision, it is a matter of carrying our appropriate assessments in advance of the processing of data, particularly the data on number plate recognition, which could be matched to individuals' names, addresses and so on. Even in advance of anything being provided for in legislation, an assessment would have to take place of whether it is appropriate to use this type of technology, and in what ways and for what purpose will the technology be used.

We have had interaction with the Policing Authority in recent years in respect of its strategy statements, and we have held meetings with it. I am not aware of the specific code of conduct or the legislation to which the Deputy referred. I thank him for that because it is good to know. On codes of practice, it is worth noting that the DPC does not have a role in making a code of practice unless it is specifically prescribed in law. Under Article 40 of the GDPR, we are tasked with encouraging codes of conduct. In this situation, we would encourage a code of conduct for community policing, to be updated, reviewed and published. It is a great document for accountability and transparency, particularly as anyone can read it and understand what the local authority or the community CCTV scheme is doing. As the committee will be aware, most communities' CCTV schemes are set up following public consultation and, therefore, there is

an opportunity for the community to raise any objections or issues with their use.

On guidance, we would assist the Policing Authority but if the guidance is a matter for it, perhaps we could ask whether it intends to do anything about it and assist in that process. From our own point of view, we are at a final stage of drafting guidance for CCTV, which I hope will be issued very soon. It will be more generic and will not deal specifically with CCTV for public sector use. To follow on, we hope to provide generic guidance for CCTV and address some of the new technologies that are being used for State surveillance or surveillance in general. We will drill down on that guidance and there will be specific guidance on CCTV for local authorities' community CCTV, and for An Garda Síochána and how it uses CCTV. That is our plan for raising awareness, setting the parameters of what type of use is appropriate, and getting the message out that when rolling out large-scale CCTV monitoring, it must done following an appropriate, detailed assessment that mitigates risk and includes safeguards to ensure that the data protection rights of individuals are protected.

Deputy Mick Wallace: I do not wish to delay our guests and, therefore, if any of my questions were not answered, the DPC might revert to the committee with written correspondence. A fellow from my office, Adrian Naughten, eats GDPR for breakfast and I will be surprised if any questions were missing. I thank our guests.

Chairman: If our guests wish to respond to any of the questions after the meeting, they might direct written replies to the clerk, who will circulate them to all the members.

Deputy Clare Daly: I, too, have a nerd in my office but some of her questions about the matter have been answered following Deputies Jack Chambers's and Wallace's points. Ms Morgan referred to 15 inquiries into tech companies, but were there not 16? Has one been completed, or were there always only 15?

Ms Jennifer O'Sullivan: Another one was opened at the start of this year, which amounted to 16. In the annual report, we referred to 15 but we opened another at the start of the year.

Deputy Clare Daly: None has been completed.

Ms Jennifer O'Sullivan: None has been completed because all of them would need to undergo the EDPB consultation process. None has even reached that stage. Given the nature of each of the inquiries, they are significant in scope. We are examining many of these issues for the first time under the legal framework.

Deputy Clare Daly: In the case of Google and France, which Ms O'Sullivan mentioned, the DPC did not take further steps because Google did not have its headquarters here at the time. Is that correct?

Ms Jennifer O'Sullivan: The complainant had submitted the complaint to the CNIL, the data protection authority in France. As Google had not yet set up as a data controller anywhere in Europe, including Ireland, it did not fall under that one-stop shop model which uses Article 60 and, potentially, Article 65, as Deputy Wallace mentioned.

Deputy Clare Daly: The DPC could not, therefore, have done much more given that it had indicated that it would follow up on Google.

Ms Jennifer O'Sullivan: We were in close dialogue with the CNIL and other EDPB members to examine the particular situation. In the original drafting of the GDPR, it was not envis-

aged that there would be a situation where a company had indicated it intended to set up a controllership but had not yet done so, and where in that intervening period a significant complaint would be received.

Deputy Clare Daly: I suppose that would not happen now. Given the scale of the breach and how egregious it was, that France was examining the matter would not preclude Ireland, as the effective European data controller at that time, from addressing it. Is that correct?

Ms Jennifer O'Sullivan: Yes. For example, if, during that intervening period, another data protection authority had received an equivalent complaint which related to the set-up process that an Android phone uses, the downstream effect on advertising and so on, it would not have been precluded from investigating it. Any data protection authority could, depending on its own national legislation, have examined the issue in its own right.

Deputy Clare Daly: I do not mean to criticise any of our guests or the commission. However, the commission has come in for some scathing criticism with regard to how it regulates the large tech companies, the multinationals and so on. In the Schrems case, for example, the assertion was that the DPC could have taken direct action against Facebook rather than taking the convoluted route via the courts, etc. People such as the former German data protection commissioner have made the point that Facebook based itself in Ireland because it can get away with murder and it is the location with the lowest levels of data protection, although I accept that we are improving and have beefed up our mechanisms in that regard. Following the shocking revelation of the close relationship with the Irish political establishment, and bearing in mind how companies such as Facebook view the Taoiseach as a puppet they can manipulate in order to secure light-touch regulation, we are in a peculiarly unique situation. On the one hand, giant multinationals are located here. Some believe that this is because of light-touch regulation but it is clear that it is also for taxation purposes. As they are located here, the DPC has become the EU data regulator, which is a challenging role. My criticisms are in no way directed at any of the witnesses because I recognise that data protection is a challenging job. As the commission is funded by Government, how does it deal with that conflict and in light of it would it be better if the commission was funded by Europe?

How would the witnesses describe the commission's relationship with the permanent government, the Civil Service? How does it work and could it be improved upon? I am conscious that in some ways this is a new role for the commission. Have the witnesses perceived a difficulty in the commission's relationship with the permanent government? I appreciate that nobody is going to admit to a committee that they a difficult relationship with the Government but in terms of accountability is there a better way in which that relationship could be managed? Has accountability emerged as a problem for the commission in the context, in particular, of the big technology multinationals and so on?

Ms Jennifer O'Sullivan: In terms of our role, which we take extremely seriously, the most serious aspect is our independence. We always seek to protect, bolster and reinforce our independence in our regulatory activities, in our work as an organisation in terms of the priorities we place on particular matters of enforcement, in the other non-investigative contexts in which we work and in the work we do on encouraging compliance. We always seek to protect that at its core. The GDPR is emphatic on the independence of supervisory authorities in general terms and in specific terms. The GDPR is the answer to the requirement for supervisory authorities to act independently. We now have one common law in Europe. A framework has been established to ensure the consistent application of that law, including in respect of the level of sanctioning and the level of decision-making in respect of the gravity and seriousness

of infringements. Deputy Wallace referenced Articles 60 and 65. There are robust and rigorous procedures in place within the GDPR to ensure that consistent application of this legal framework. Article 65 has not been put in practice yet. We have had fewer than ten Article 60 decisions across the EU achieve completion. The EDPP is very much still testing the waters of these procedures.

In summary, the framework is in place to ensure that every data protection authority in Europe is applying the law consistently and in its findings.

Deputy Clare Daly: It is difficult to do that when the law is new. Have any red flags emerged in respect of what we might need to do legislatively, for example, to beef up the independence of the commission, or are the witnesses satisfied that teething problems aside everything is working out?

Ms Jennifer O'Sullivan: The situation is as challenging as we expected given there is a new legal framework and, simultaneously, data protection and privacy is now part of public discourse in the mainstream whereas a few years ago it was not. Regarding our budget and funding, this year the commission will become the Accounting Officer for its own funding. We will be separate from the Department in that regard from next year, and we will have our own Vote. It is not that this speaks directly to our independence as a supervisory authority but it further underlines our independence as an organisation. This change will occur in the coming months.

Deputy Clare Daly: The commission has the power to levy fines under the new legislation. As I understand it, no fines have been levied yet. Given that none of the investigations would necessarily be terribly complex or long-winded, why have no fines been levied? Is the commission satisfied that none of the cases which have been concluded met the threshold for a fine and how much discretion does it have in that regard? Have there been internal discussions on whether a fine should be levied? We see fines as an effective mechanism for correcting behaviour. A strong signal tends to get the message out.

Ms Anna Morgan: In regard to fines, there is a particular process that must be followed as set out in the legal framework established under the 2018 Act. There is a decision made in the context of a statutory inquiry that is opened under section 10 and that decision is on whether there has been an infringement of the GDPR or the 2018 Act. The next step which the commission must take in exercising its decision-making power is to decide if there has been an infringement the type of corrective power that should be imposed. As the Deputy mentioned, administrative fines are one of a range of corrective powers that can be imposed by the commission. These corrective powers are the same across Europe.

Regarding the process that has to be followed, earlier I referred committee members to the statutory inquiry process we have outlined in our annual report. It is important to underline that. There cannot be any short cuts taken in the statutory inquiry and the decision making that occurs at the end of that inquiry. Ultimately, our decisions as a quasi-judicial body must be robust and legally sustainable. There are extensive powers in terms of judicial remedies that are open to any party that is impacted by our decision. We are mindful, in having plotted out those procedures over and above what is in the 2018 Act, that we must take full account of the right to due process and to fair procedures, which are all referenced in the GDPR as well. As I said no short cuts can be taken in regard to our inquiries. It is a process that must be followed. Once the fact finding stage has been completed and the analysis of the facts has been completed and the official decision-making function has been carried, out the end point will be a determination as to whether a corrective power or administrative fine, among others, should be imposed.

I refer the committee to Article 83 of the GDPR, which sets out the circumstances that must be taken into account by a data protection authority when determining the level of fine that should be imposed where there has been found to be an infringement of the GDPR. Of particular importance in this regard are issues such as the nature, gravity and duration of the particular infringement. The GDPR also emphasises that the purpose of administrative fines is to be effective dissuasion. They must also be proportionate. These are all factors which will be taken into consideration in the context of the decision-making phase, which will come after the investigation phase of our statutory inquiries concludes.

Deputy Clare Daly: Ms Morgan's response does not address the question. My question started when her response ended. I am speaking specifically about cases which the commission has concluded fairly in accordance with the legislation. I know that the commission has identified breaches. In the context of all those cases the commission fairly and transparently investigated, there was no case in respect of which the commission deemed it necessary to impose a fine. How many of those cases met the threshold for a fine and were fines discussed in that context? As I said, we see the imposition of a fine as an effective remedy.

Ms Anna Morgan: It is important to distinguish between the complaint handling function that we perform, which relates to the vast majority of issues that come into the office, and the statutory inquiry. In terms of complaint handling, our obligations under the GDPR are to handle a complaint and investigate it to the extent appropriate. In complaint handling we are always focused on vindication of the data subject's rights. It may be that having concluded a complaint handling function and having obtained an outcome for the individual we then go on to consider whether issues that had been raised in the context of that individual complaint are systemic to the data processing operations of a given organisation or pose a particularly high risk to individuals who are also users of services or products of a particular organisation. There is a decision to be taken by us as to whether it is appropriate, when we are faced with a set of circumstances that might indicate systemic or high-risk issues around processing, to commence a statutory inquiry.

It is in the context of statutory inquiries that we can impose administrative fines as a range of corrective powers and, as I referred to, 49 statutory inquiries have been opened by us. In that context, it is open to us, at the end of a statutory inquiry wherein we have found one or more infringements, to impose a corrective power or another administrative fine.

To contrast that with complaint handling, we can use a different range of methods to close off complaints. We might issue advice to the data controller if we find that a company's systems are not necessarily compliant with the GDPR but the complaint lends itself to amicable resolution or to another of the different types of outcome that are contemplated by section 109, which sets out what steps we can take in handling a complaint.

Deputy Clare Daly: Perhaps I am misunderstanding and I am sorry if I am. Is the answer that it is only the statutory inquiries that give the commission the power to fine and, as none of those has been completed, there have been no fines?

Ms Anna Morgan: That is right.

Deputy Clare Daly: That is the answer. I was a bit scared about some of the points made about the public services card, PSC, investigation and found the responses to Deputy Wallace's questions a little bit chilling. The commission has been investigating this since 2017. The witnesses have said that things have moved on and the issues relating to driver's licences and so

on have been sorted. In fairness, the commission identified, well over a year ago, the illegal basis upon which the Department was operating the PSC. We know, as a result of the dialogue in society, a number of changes have come about, but those are not as good as they should be. Let us be clear that the Attorney General gave a legal opinion which, this time last year, led to the Minister for Transport, Tourism and Sport telling the Road Safety Authority, RSA, not to rely on the PSC for driver's licences but it still kept doing it for another five months, in flagrant breach of that ministerial instruction.

The Data Protection Commissioner said this was a pressing matter which needed urgent attention in August 2017. Our systems needed to be sorted at that stage. Here we are in April 2019, and it has not been concluded. I do not get that. I note the exchange the witnesses had with Deputy Wallace about the full report and I am not entirely clear on that. I am not clear why it has been delayed. The Department gave the commission 470 pages that have to be analysed. That seems like a general sort of Civil Service approach to inquiries - dump a pile of information late in the day and bog people down in that sort of stuff. That said, 470 pages is not an enormous amount, given the time this investigation has been going on. When can we expect it to be concluded? I know the witnesses said the commission does not have the expressed powers to publish but do they think there is a legal impediment to publishing, or did I understand the witnesses correctly in replying to Deputy Wallace that the commission would have to get the permission of the Department to publish the final report? I was not fully sure on that point.

Ms Anna Morgan: It is the position that the commission would have to consult with the Department to confirm that it consented to the publication of the full report.

Deputy Clare Daly: And if the Department does not consent, the commission cannot publish.

Ms Anna Morgan: As I said previously, we intend to publish a summary of it which we believe is necessary in the public interest.

Deputy Clare Daly: I know that but we would like the full report published. Is it Ms Morgan's understanding of the legal position that the commission must get the permission of the Department to do that?

Ms Anna Morgan: That is our understanding of the legal position and it is the position we have applied in relation to other reports, including audit reports, which we have conducted over the years.

The Deputy made comments about the time the inquiry has taken. I reiterate some of the comments we made previously and outlined in the annual report that there are a range of quite complex legal issues under consideration in the context of that report. We have considered a vast volume of information, both publicly available and provided to us in the context of those submissions. That includes information that has come not only from the Department itself but information we have had to consider in the context of the use of the PSC by other Departments.

In connection with the further steps to be taken, it is vital that we follow fair procedures in each and every inquiry and investigation that we conduct and do not short-circuit those procedures. That involves allowing the right to be heard to the party that will be impacted by any decision or outcome of our investigation process. That applies as much to Departments as it does to any private or commercial actor. The need to allow the opportunity for submissions to be made where there might be findings in respect of the law is an essential element of the steps

we have to take in any investigation or inquiry.

Deputy Clare Daly: I do not think anybody would accuse the commission of short-circuiting or not giving enough time, given the fact that the Data Protection Commissioner is on record in August 2017 saying that she, and presumably her staff, had conveyed their views "on numerous occasions to the Department of [Employment Affairs and] Social Protection and in a number of fora" that there is a pressing need to deal with this. There is no short-circuiting. This has been going on a long time. The indications were that the report would be finished in April 2018 and it is now April 2019 and there are serious issues relating to it.

Do the witnesses know how many bodies are using the SAFE 2 PSC system and how many of these are requiring that this be the sole form of acceptable identification? I do not expect the them to know that but would they be able to provide that information to the committee later? That would be helpful.

Ms Anna Morgan: I do not have that information to hand but we will certainly consult internally on those issues.

Deputy Clare Daly: It would be brilliant if Ms Morgan could do that. In a recent reply to a parliamentary question, the Minister for Employment Affairs and Social Protection reiterated her view and, I suppose, that of the Department that a SAFE 2 PSC photograph is not itself biometric in nature and that the Department does not collect or share biometric data. Do the witnesses agree with those two statements?

Ms Anna Morgan: In the interests of preserving the integrity of the process we are involved in at the moment, I will say that is being considered in the mix in the context of our investigation and against the backdrop of the information we are considering.

Deputy Clare Daly: Those issues are part of the process that is under way.

Ms Anna Morgan: They are.

Deputy Clare Daly: The witnesses might have answered this question during the one minute I was outside the room and, if they did, I apologise. Deputy Jack Chambers raised questions about the digital age of consent which was set at 16, despite our best wishes and those of every single child protection expert in this State. One of the main movers who advocated behind the scenes to raise the digital age of consent to 16 from the originally accepted age of 13 was an adviser to, and quoted by, some members of the Fianna Fáil Party who are not in attendance. That person is now involved in a private company, which is seeking to produce patented age verification biometric technology, something for which a larger market was created when we raised the age of consent to 16. That is interesting and not surprising.

Leaving that aside, how is the age of consent being implemented? How is the age being verified? Does the commission know if companies are using technical fixes or what is going on with that verification? I know that in the US under the Child Online Protection Act, COPA, companies are asking parents to scan copies of their credit cards or Government IDs or whatever. Is anything like that happening here? What is the role of the commission in that? I am aware that a consultation is under way.

Ms Anna Morgan: The consultation is central to examining these issues. We will pose the question of what the appropriate age of digital consent should be. We noted the representations made by various charities and children's representatives. Under section 31, a review of the age

is to be carried out after three years and we hope the consultation exercise will provide us with valuable feedback on the opinions of stakeholders. That is connected to the exercise of children's rights, which is another pertinent issue under the Data Protection Act.

On the question on the operation of the age of digital consent, there are mechanisms such as age gating, which organisations use to verify children's age by asking for a date of birth, and giving only a certain number of attempts to demonstrate that they are over the age of digital consent. Lots of different sectors and jurisdictions have struggled with this and we are examining how to implement an effective age verification method, bearing in mind that when a platform tries to collect the age of users it will lead to the collection of age information on all users, which raises issues around the excessive collection of personal data under the GDPR provisions. They are complicated issues and we are hoping our consultation will throw some light on what may be best practice for organisations.

Deputy Clare Daly: It is very challenging and raises major data concerns, such as over the possibility of hoovering up parents' data. One proposal was to scan children's retinas to verify their age, which is mad and scary. Have any breaches of legislation been reported to the commission in the area of age verification?

Ms Jennifer O'Sullivan: The Deputy mentioned the COPA Act in the US, which has been in effect for approximately 20 years. The methods of verifying age which have been found culturally acceptable in the US have not gone down well in Europe. We have had complaints from parents who have been asked to provide information which they consider interferes with their privacy. We have not identified breaches but we have received complaints over the method of verification.

Deputy Clare Daly: Could the commission investigate these further or does it need more legislation? Perhaps the data has not been processed yet.

Ms Jennifer O'Sullivan: We are looking at the complaints but they are cases where the parent's or guardian's privacy has been impeded or infringed. We have not received complaints that an organisation offering online services has not attempted to verify age.

Deputy Clare Daly: This was something we warned about when we lost the battle on the age of consent being 13.

Chairman: For clarification, when the Deputy referenced me on the age of consent, she referred to all of us who remain on the committee.

Deputy Clare Daly: Absolutely. My final point is about data subject access rights and the gardaí. Does the commission have any role in respect of data held by gardaí? There have been a number of cases where people have sought information about themselves from gardaí but did not get the full facts, supposedly for security reasons. Is there anything people can do or anything the commission can do to help people in these circumstances? I am aware of people who did not get a job as a result of a Garda vetting operation and, while they got some information back from gardaí, other information was denied to them on security grounds. They believe this to be erroneous and if they knew what the information was they would be able to challenge it. They are pretty sure they never did anything to warrant being blocked. There must be some way around this.

Mr. Cathal Ryan: We are looking at the whole vetting procedure and at what is and is not disclosed, and we are looking to update guidelines in line with the GDPR provisions on Article

10 data, which relates to allegations of criminal activity and offences.

We look at subject access requests following a complaint or through an audit. We can look at the individual complaint and ask what information is not being shared and we can carry out an inspection to determine whether the test for non-disclosure of the full set of data was applied correctly. In the past, gardaí may not have disclosed certain information that could have prejudiced the investigation of a case. We have to look at what data are not being disclosed and make a determination on that. It is difficult to do so without the necessary knowledge.

The Garda Síochána has a very good data protection unit, which was set up following the GDPR. Internally, the unit would need to oversee how requests are being handled. It would not be one individual garda who would make the call and it would have to go through a certain procedure.

Deputy Clare Daly: Can a person get to see his or her full file?

Mr. Cathal Ryan: Yes, if it is required. An audit is a more rounded inspection of what is going on in terms of procedures. It would depend of the terms of reference but if a complaint was made following an impasse, we would probably have to carry out an inspection to get the information.

Deputy Clare Daly: I am trying to establish whether gardaí could hide behind national security considerations.

Mr. Cathal Ryan: It depends on what is in play. If State security was the argument being made, it would probably fall under old legislation, namely, the 1998 Act. Typical Garda operations fall under the law enforcement directive. We have powers to carry out investigations and inquiries. If an individual feels he or she is not getting access to data for whatever reason, such a person can make a complaint and we will then have to handle it.

Deputy Clare Daly: Is it the case that there is no impediment to the Data Protection Commission asking gardaí? I am thinking of a particular case where people were denied information and we have heard of a number of tragic cases where people applying for citizenship have been told to come along to the ceremony, only to get a letter shortly before the event telling them it is being postponed. They ask why but are told the organisation has received information and is looking at it. They can never see what the information is, however. We have seen monumental evidence of it and I know the Chairman is involved. Could our guests see what this is because we are just told "Oh, we've heard something and we're looking into it"? This could go on for years and the person is-----

Mr. Cathal Ryan: It is a very difficult situation for individuals. We are all about ensuring that individuals have the right transparency concerning how their data is processed. That is a significant piece of work in which we are engaged in terms of ensuring that information notices are clear and people are aware of how their data is being processed. It relates to the recommendations of the Murray report. I know the latter concerned surveillance and telecommunications data but it relates to ensuring there is proper oversight. If someone is stating that data cannot be shared on the basis that it will prejudice a case, how we do know that? What notification has been mentioned? What authorisation has been given? An Garda Síochána has those checks and balances in house but in respect of an individual who wonders why it possesses something it is not sharing with him or her, a complaint could be submitted to our office or a query could be sent for us to check. We have that relationship with An Garda Síochána. We work with the data

protection unit of An Garda Síochána all the time. A lot of what An Garda Síochána is doing involves updating its systems. It has implemented a really robust assessment package so much of what it does is underpinned by data protection impact assessments. An Garda Síochána is really implementing the law enforcement directive in full in terms of its assessments, the appropriateness of assessments and all of its procedures. So there will be checks and balances internally to assess whether it is doing things right but, obviously, if an issue arises where an individual feels he or she is not getting all of the data for which he or she has asked, there is recourse to figure out whether the law is being applied in an appropriate manner.

Deputy Clare Daly: That is really helpful. As if the DPC is not busy enough, which I know it is, it will be busier now as a result of opening that door.

Mr. Cathal Ryan: That is the point of what we are trying to do. Obviously, there may be an individual case but we cannot just suddenly run for every individual case. We have to learn from that case and then apply a standard of what is expected in order that we do not receive any more complaints. Engagement is about trying to get that message across. Let us get it right before the fire starts.

Deputy Clare Daly: I thank our guests and look forward to the other answers that will come later.

Chairman: Deputy Clare Day stated that a number of her questions had already been asked by colleagues. She has done the same to me in respect of the Irish Naturalisation and Immigration Service, INIS. I would like confirmation that INIS is accountable to the DPC regarding any issue that the commission wishes to raise and that those who are applicants for consideration by INIS in terms of their status and standing in this jurisdiction are also entitled to the same protections as citizens. Is that the case? Yes. I thank our guests for that.

It was stated that the DPC's remit as a regulator applies regardless of industry. Reference was made to the 15 inquiries relating to the multinational technology sector and that a further 33 domestic statutory inquiries are under consideration. They have been referred to during the course of the exchanges here this morning. Do any of those domestic statutory inquiries apply to any of the banking institutions functioning in this jurisdiction?

Ms Anna Morgan: There are 33 domestic inquiries, 31 of which relate to the CCTV investigations we have running in respect of to the use of CCTV and other types of electronic surveillance by local authorities. Of the other two inquiries, one relates to a series of data breach notifications made to us relating to Tusla so we are examining the security issues around those data breach notifications.

Insofar as the financial sector is concerned, we certainly receive an awful lot of complaints from consumers regarding banks and insurance companies in particular. Data breach issues constitute a very salient issue for that industry. A very large proportion of the data breach notifications we receive relate to banks and insurance companies. It is something at which we are looking to decide whether or not there is merit in opening statutory inquiries of our volition rather than inquiries being complaint-led with regard to that ongoing stream of breach notifications. From analysing the breach notifications that come to us, we can see that organisational security measures remain a really big risk and a very large number of breaches relate to disclosure that really should not have happened. An example would be a bank statement or an insurance policy being sent out to the wrong address or an old address. That is something we are actively targeting in terms of further statutory inquiries on the domestic front.

Chairman: This is an area that needs to be addressed and not only in the context of the forwarding of material to incorrect addresses. There is a much more serious issue. I use the word "domestic". The selling of mortgages is a significant issue of address in these Houses. What does it entail? It entails the selling on of all of the data that is relevant to the borrower. Regarding a borrower presenting to any financial institution, the experience heretofore would have involved a high-street engagement with the local presence of any of the banking institutions. There is a knowledge and recognition factor and while a lot of the decision-making has been centralised and taken away from the high-street representatives of the respective banking institutions, the fact remains that, regardless of the small print, the people signing up for these arrangements had no idea that their information would have been available for sale on the market to vulture funds. A number of people have reflected their great upset and disquiet at this. Let me underscore that there should be no distinction because it is an issue that needs to be substantively addressed but we should not for a moment believe that the main banking institutions are just selling on non-performing loans or under-performing loans. For whatever reason, they are selling on fully performing loans. That is a fact. Somebody enters into an arrangement with a banking institution and signs off to borrow to purchase a home or whatever might be the case and his or her loan is performing in line with the agreement with the bank throughout. This person can then find himself or herself being notified by the bank that it is selling on the loan. The person then appeals the decision and the appeal is rejected. As someone who formerly worked in a banking institution in this country, I can attest that this is the case. This is a really vexed issue. I cannot emphasise enough that selling on a loan involves selling on the individual data in tandem. It is being sold as a package. We do not even know if the information is retained in the jurisdiction. Invariably, that is not the case. Vulture funds *et al*. are international operators and that is not what people here understood they were getting involved with in the first instance. This is a very serious issue. I urge the DPC to give serious consideration to addressing this. I will not put a tooth in it, but, in my opinion, there are flagrant abuses, including of the nature I have just recounted. It is inexplicable, which is all I can say in that regard.

Our guests indicated that rather than reacting to a request, the commission might initiate a statutory inquiry. How are statutory inquiries initiated? How are they carried out? Is it of the commission's own volition or is there a request process that has given rise to the 33 domestic statutory inquiries currently in train and will give rise to any in future? Can the methodology employed be clarified?

Ms Anna Morgan: There are two types of statutory inquiry we can process under section 110 of the 2018 Act. We can take one of our own volition or we can commence an inquiry which is complaint-led. There are a range of factors which will influence our decision on whether to commence an inquiry of our own volition. For example, if we see trends or patterns which point to particular issues within a sector or specific organisation and which raise wide-scale concerns regarding the processing of personal data, in other words if systemic issues are pointed to, it will factor significantly into a decision on whether it is appropriate to open an such an inquiry. Factors include volumes of data subjects being affected along with different types of processing operations and the different types of data being processed. Obviously, there are special categories of personal data that merit particular protection under the GDPR.

If there are certain subsets of data which fall into the mix and which pose higher risks to the rights and freedoms of individuals in the context of data protection, that is an issue which will weigh heavily on our decision on whether to commence a statutory inquiry. Equally, it is not just trends in complaints submitted to us that have a bearing on how we decide where to apply the significant resources required to carry out statutory inquiries. We may have indica-

tions from civil society of a belief that there are issues with a particular organisation or sector or industry. There are a number of privacy advocacy groups that are very active in this area. Equally, issues may be brought to our attention by the media and, of course, elected representatives also. There is a range of sources from which we can be alerted to particular issues, including our own internal monitoring of issues, breach notifications, complaints and trends raised by queries submitted to our information and assessment unit. All of this is factored into the mix.

Chairman: I thank Ms Morgan for that. There was a reference to policing to which Mr. Ryan responded. As a committee, we have given dedicated address in the course of this year's series of hearings to the whole post-Brexit situation. Does the commission anticipate any impact on its role with the advent of Brexit, whether by crash-out or agreement? From a justice perspective, we have had representatives here from An Garda Síochána and the PSNI. Are there implications for cross-Border policing and co-operation and the sharing of information on individuals in the event of the worst-case scenario presenting? Data protection and data sharing are a critical part of the co-operation between the two police forces on this island and have wider implications. A committee colleague and I represent our parliamentary institution on the EU oversight committee relating to Europol. It is not something I expect that our guests will be able to comment on immediately but it is an important matter. I am looking at it from the domestic point of view - that of the island of Ireland. Is it something the commission has considered? What our guests tell us?

Ms Jennifer O'Sullivan: I might answer the question on Brexit generally first and then hand over to Mr. Ryan to speak directly to the exchange of information between policing authorities on the island and across Europe. The commission has been engaged heavily in Brexit preparations for the past several months and it is an active topic of conversations with colleagues in the EU at the EDPB. The transfer of personal data outside the EU is a central element of EU data protection law and is taken very seriously because the relative standard of protection for personal data is so high in Europe. To not have those safeguards in place would undermine that standard. The DPC has been issuing guidance to organisations that seek to transfer data from Ireland to the UK. Over the past several months, we have being doing that and it has also been done via the Government's communications channels. The EDPB has also been issuing guidance on that. We are also working with our UK counterparts in preparation for the potential impact on live cases that are cross-border in nature. On the transfers question, there are several mechanisms available for the transfer of personal data outside the EU. If the UK leaves without a withdrawal agreement, it will be considered a third country. For regular organisations, the simplest and quickest method to utilise will be standard contractual clauses. We have templates for those on our website. There are some organisations which choose to use a mechanism called "binding corporate rules". When it comes to transfers by public bodies, particular provisions are in place and the DPC has been involved recently in authorising some of those as required by the GDPR. Mr. Ryan might speak specifically to the question of the exchange of data in a policing context.

Mr. Cathal Ryan: Brexit is on everyone's mind and that is certainly the case in our office. We are receiving the legislation or administrative arrangements that follow Brexit. It is an ongoing consultation on the different arrangements being put in place. On the policing side of things, the framework is there in the Data Protection Act. Sections 96 to 100, inclusive, set out the parameters within which one can share data. Without getting into the specific provisions, there is first of all no adequacy decision in place, which is something the commission can approve. That is something that may come later. The big thing in relation to the sharing of data is to ensure the same safeguards and rules apply when one shares data to a third coun-

try. Standard contractual clauses do this. However, administrative arrangements can also be put in place which, provided they are appropriately specified, can actually act as another way to ensure appropriate safeguards are implemented. They can ensure there is a similar level of protection for the data in the third country as is provided for in this country. For example, we are currently analysing whether those safeguards are put in place. Rather than just one line, it gets into a very detailed level of what data is being shared and how and what oversight there is of that data. Provided these safeguards, of which there are many more, are implemented, we take a practical view of Brexit.

We have a long-standing relationship with the UK. Mutual assistance has been in place for quite some time, albeit it will fall by the wayside in Brexit. It is very important to note, however, that there is a data protection office in the UK, namely the ICO, which has been a leader in the field of data protection. The ICO is heavily involved in data protection at an EDPB level but it will have to leave the board on foot of Brexit. The ICO has nevertheless been at the forefront in implementing a law which brings all of the provisions of the GDPR over into English legislation. Obviously, there will be some divergences due to sovereignty if Brexit happens, but the core elements of the protection of data are there. There is oversight and there is a regulator in the ICO. As such, we have to be very pragmatic and understand that these structures are already in place. It is really a matter now of deciding what level of data is being shared, how it is being shared and what level of oversight there will be of the sharing arrangements. Something else one will note, especially when one looks at which provision they go for, whether it is section 98 or 99, there will be a function for the DPC in terms of ensuring that reporting requirements are fulfilled. We could inspect whether the documentation that is being shared is appropriate, in line with the administrative arrangements or whatever arrangements are put in place. There will be a proactive involvement of the DPC in terms of monitoring those sharing arrangements.

I go back to the fact that our friends, the data protection officer unit of the AGS will be well aware of these provisions. They will be trying to figure out which is most appropriate to them, in terms of their everyday work and in terms of their interaction with the UK. Clearly, they are the ones who will make the decision and we will help them in that decision in terms of what is required, what level of data needs to be shared, and the date and time of the transfer. Retention is also a big issue. I refer to ensuring that if one shares it to a third country, it is not then shared beyond that third country, and if it is, how is it being shared beyond that third country, etc. There is a level of transparency required which is appropriate to the function of the AGS and we would be the body that would reflect and review those data-sharing arrangements under section 98 or 99 of the Data Protection Act.

It is very possible. We have to be pragmatic, given Brexit. The Commission, the EDPB itself, from a general data protection regulation standpoint, has effectively stated that we need to look at how derogations would be used. Ultimately, if we are looking at some form of derogation, it is never the solution. We should be looking for a more permanent solution. Obviously, the Commission and the UK may in the future look at an adequacy decision which would clear this matter up. In the interim, we should not be relying on a derogation for the next four or five years until something like that happens. We would need to probably set in motion some more permanent solution rather than simply relying on a derogation for every data-sharing arrangement.

Chairman: I appreciate that very much. I welcome the fact that this is an issue that the Data Protection Commission has been addressing. It is important. Here we are on the cusp perhaps and it is quite alarming to find where there are so many gaps that people are only just saying,

"Oh my goodness, what should we be doing." This will impact right across the board. People do not have a sense of the scale and scope of this. It will be significant.

I have bunched together the last little couple. In that last reply, Mr. Ryan talked about regular engagement with the different companies, for example, the multinational technology sector. What does the Data Protection Commission's engagement with them entail? I will explain what I have on my mind. In terms of the HSE, I have HIQA in mind. Is the Data Protection Commission a HIQA? Does the Data Protection Commission carry out unannounced visits in terms of its audit, inspection or inquiry? Give me a sense of the nature of this relationship with the Facebooks of this world? Does the Data Protection Commission carry out unannounced visits or is that simply not the way it works?

Ms Jennifer O'Sullivan: Our relationship with these big multinational technology companies is multifaceted. At the hard edged enforcement side of it, we have our statutory inquiries that are open. I mentioned that we have not considered those to be investigations, which give us more powers, and we have not used unannounced inspections in those inquiries to date. The nature of the engagement with these companies on these particular statutory inquiries is quite formal. There is a significant amount of correspondence which relates to the fair procedure that we must adopt in these inquiries. Ms Morgan mentioned the right to be heard, the requirement for these organisations to be allowed to make submissions at the various stages of the investigation, and it is quite a formal written type of engagement when we are engaging with them in that context.

Separately, the GDPR introduced a requirement whereby where an organisation is considering introducing new processing that requires personal data to be processed, it must carry out a data protection impact assessment and it must mitigate the risks that are associated with that. If it finds that it still, for business or whatever other social reasons, wants to carry out the processing in the future but it has not been able to mitigate all of the high risks, it is obliged to come and speak to us. That is a different kind of engagement, which is quite formal in its own right.

Separately, we engage quite formally with these organisations when we receive intelligence, media reports or submissions that are brought to us, I suppose, in a pre-inquiry stage. That kind of engagement would be a combination of the following kinds of dialogue: in-person meetings; written correspondence; and us reviewing submissions they make to us on the matter.

We would have other reasons to meet them. Perhaps they want to give us an update on their general data protection activities. Particularly in the lead up to GDPR, we would have had several meetings with the big companies in that context whereby they wanted to give us an update on their preparations for the GDPR. Those would generally have been in the context of meetings where we had a discussion with them. They might bring to our attention new products that they were considering or that were further down the line, and we would have that kind of engagement with them in that context.

Chairman: The unannounced visits have not started yet.

Ms Jennifer O'Sullivan: We would have to examine in the context of a particular inquiry whether there would be value to it.

Chairman: I appreciate that. The following is absolutely the last one - I am getting worse than Deputy Clare Daly.

In the course of Ms Morgan's address to us at the outset, under "New trends", she stated that

in light of the requirement on the Government to consult the DPC on certain new legislation, the DPC has reviewed and provided "observations on new and draft legislation, with 25 items of primary or secondary legislation coming to the DPC for review during this seven-month period", I guess, from the inception of the GDPR to the end of the year. As to new and draft legislation, the largest body of legislation that goes through these Houses is scrutinised in this committee. We take Committee Stage of the greatest body of legislation passing through the Houses, that from the Department of Justice and Equality. The requester in this instance, I presume, is the Department. While I could understand the Data Protection Commission's responses going on the draft which may not have even presented in the general scheme coming before the committee, when I hear the point about new legislation I note my colleagues and I are the legislators. Ms Morgan indicated 25 items to which the DPC has responded. Government may be the initiator but I, as Chair of this committee, have no recall of ever having received any feedback on legislation from the DPC. I wonder is that the way it should be and is that appropriate, if we are not the requester. Legislation is the business of the Houses, the Dáil and the Seanad. Deputies Clare Daly and Wallace initiate legislation. They are called Private Members' Bills. We deal with them all the time. Government sponsors Bills. We deal with them all the time. I would have a degree of confidence that if Deputy Clare Daly had requested a DPC opinion on a piece of legislation, the Deputy would share it, and if it was new legislation that had got to Committee Stage, it would not be withheld from us. I do not see why Government should be different because it is the initiator of proposed legislation from those of us who are broadly labelled or perceived to be Opposition voices. Perhaps the commission representatives would comment on that. My own sense is that if the commission is there to carry out a specific function then we, as legislators, should be privy to all the relevant information to inform us as to the suitability, the consequences and the concerns - if any - of all legislation. I do not believe that anything should be withheld from our eyes. As the people who make the law, members have a statutory responsibility and a public role and responsibility. In responding to such requests in the future would the commission think it appropriate to release its replies to the Members of the Houses or the respective committee? I believe it should be the widest possible audience. How would the representatives like to respond to that?

Mr. Cathal Ryan: The Chairman makes an interesting point. When we say 25 pieces, our function is set out in article 36 of the GDPR with regard to consultation that happened prior to a legislative or regulatory measure on foot of a legislative measure. It has to happen in advance of the processing of data. The appropriate timing for that consultation with us is really a matter for the Department or, if it was a Private Members' Bill, for the individual who sponsors the Bill to determine when is the appropriate time to consult with the data protection authority under article 36. To be fair, anecdotally it is the case that individuals or Departments are coming to us early - almost as a policy and as a sketch of where they feel the legislation is going. They know there is movement in terms of legislation, and while it may not have gone to the heads of a Bill, they may be worried that at a heads of Bill stage the policy approach is simply a red-line issue for the Data Protection Commission, DPC.

Sometimes, appropriately, they come to the DPC early to see that general approach taken by them will not contravene data protection law. The figures we have presented incorporate some of those engagements, which are at a very early stage in their processes, almost at the policy development stage.

We are very happy to engage at that level because there is no point in them going down a rabbit hole of data protection and for us to then turn around at publication of a Bill and say their situation is untenable.

We have previously looked at publishing all of our replies, but the problem is that our replies may have to be collated together over a period of time to get an overall sense. We may, for example, only get a question on a specific policy approach that is intended to be given legislative underpinning. Instead of looking at a heads of Bill, a piece of legislation or a whole Bill we may sometimes only get a policy approach on where a body is going and we would be involved at that level. We have looked at consultation and publication of our responses because not only would it help the Department it would also give transparency, and other Departments would learn of the particular approach taken or the way a data protection authority has viewed a certain matter.

With the creation of online registers for a public sector body, for example, in the recent past we have given observations many times on our views around the creation of online registers and the publication of same on websites. Instead of only the recipient of those observations learning from that, I am very happy to share them out. We would need to set up a process or format for how and when we do that. It comes back to when it is appropriate or when is the perfect time for a Department or a Member to come to us to get a full overview of our position, rather than a piecemeal effort that is almost out of context.

I note that we have been invited before by this committee during a pre-legislative scrutiny. If we make observations they are collated and shared currently through the Department of Justice and Equality, but we would also make our own observations as an independent authority in the future. We would look at how we might publish our observations for everybody's benefit. This is something we had considered prior to GDPR. We have also looked at other authorities in Europe and elsewhere, including around consultation about a project or initiative. The New Zealand data protection authority firmly states that it may publish its views on a project.

We must also practise what we preach with regard to transparency. If we are to demand transparency from everybody then we too must be transparent. From my perspective, consultation would be great because we would get our message across to the person who has asked the question and also to the wider audience. This is very important because it would help with understanding, awareness and a standard approach to data protection that would meet the requirements of GDPR or the law enforcement directive. I am very much open to suggestions on how that can be done effectively. I would not walk away from that. It is important. This could offer another access to information along with freedom of information requests - which we receive only under administrative functions and not necessarily for investigations and so on. These are important issues with regard to the data protection viewpoint. It is to our own benefit that by publishing our views of these matters they do not get hidden within everybody else's observations: we can highlight what the particular issues are for us. As legislators the Members would also be aware of the views of the DPC while they go through the various stages of the process in the Houses.

Chairman: Be it either detailed scrutiny or pre-legislative scrutiny, as the case might be, and whether it is Government or Private Member initiated legislation, the critical element for us in carrying out our functions is that we need to be fully informed. I listened fully to Ms Morgan's address and I thought it was interesting that I have been chairing this committee since 2016 and I have never seen any of the responses that were referenced. I am sure my colleagues would concur that this is also their experience. It is not that we want to look into their copybook. We want to be the best we can be in the service of the people who have entrusted their vote to us to perform here.

The point was made that the DPC has responded to scrutiny of 25 pieces of proposed legis-

lation. Was any of them a Private Members' Bill?

Mr. Cathal Ryan: No. One was actually a Bill that was almost piggy-backing on a Private Members' Bill. Sometimes the Bill may not go through pre-legislative scrutiny so it is really determined by that. I have absolutely no problem sharing our observations on legislation that is going to see the light of day or which will come to this committee. It would be a matter of engaging with us to figure out the appropriate timing for that. I do not see anything preventing us from doing that, as long as all parties are aware that we may publish. Not everything will be published. Sometimes we come back with nil observations because we simply had no observations to give. When, however, there are important data protection implications to legislation then I am very happy to do it, if we can do it. I am surprised that the committee does not get sight of our views on the legislation.

Chairman: It is worth noting. The reason I have raised it is to ensure better communication, transparency and ultimately better legislation because that is our function here in the first place.

I thank Mr. Ryan, Ms Morgan and Ms O'Sullivan on behalf of the committee. It has been a very worthwhile engagement. The DPC is not even at the first anniversary of GDPR yet; there is another month to go. By this remark I am signalling that we will do this again at some point in time down the road. Go raibh míle maith agaibh arís. I also thank my colleague members for staying the course.

The joint committee adjourned at 12.10 p.m. until 9 a.m. on Wednesday, 10 April 2019.