



Select Committee on the European Union

Home Affairs Sub-Committee

Corrected oral evidence: The EU Data Protection Package

Wednesday 8 March 2017

10.45 am

[Watch the meeting](#)

Members present: Baroness Prashar (The Chairman); Baroness Browning; Lord Condon; Lord Cormack; Baroness Janke; Lord Jay of Ewelme; Baroness Massey of Darwen; Lord O'Neill of Clackmannan; Lord Soley; Lord Watts.

Evidence Session No. 3

Heard in Public

Questions 22 - 41

Witness

I: Elizabeth Denham, UK Information Commissioner, Information Commissioner's Office.

Examination of witness

Elizabeth Denham.

Q22 The Chairman: Good morning and thank you very much indeed for your time this morning. As you are aware, this is a public session and it is being webcast live. You will be sent a transcript of what you say and be given the opportunity to correct it if you so wish. At that stage, if you feel you want to send us further written information, please feel free to do so. I understand you want to make a statement before we get into the questions.

Elizabeth Denham: Yes, thank you. I have a very brief opening statement. Good morning, everybody. I am very pleased to be here and am very happy to accept the invitation to contribute to the work of this Committee. As some of you may know, I am very new to the job of Information Commissioner; I think this is my eighth month. However, I did similar regulatory work in Canada for a dozen years. My role is to safeguard the public in terms of privacy and data protection and to administer the data protection law, the freedom of information law and the Privacy and Electronic Communications Regulations in the UK.

I find, though, that this is increasingly an international job, because data knows no borders. When the UK leaves the EU, we will still need an effective, harmonised and high level of control and protection for citizens' and consumers' personal data, to ensure the free flow of information for appropriate purposes, such as international trade, but also to provide essential protections and incentives for all sectors, including the law enforcement sector. The post-exit regulatory framework is in the Government's and Parliament's hands. I am a creature of statute, but I am also an expert adviser to Government and Parliament. I have opinions, but at the end of the day I regulate the law that is in front of me. I hope I can be of assistance to you today.

Q23 The Chairman: I am sure you will be, because it is a subject that, as you know, is extremely important and has international significance. We are looking at four elements of the EU data protection package, which are the General Data Protection Regulation, the law enforcement directive, the EU-US Privacy Shield and the US-EU umbrella agreement. It would be very helpful if you could outline for us the implications for the UK in terms of the impact on data controllers—that is, employers—and data subjects. Can you give us a broad indication of the implications?

Elizabeth Denham: Yes. There are four pieces of the package. The General Data Protection Regulation and the law enforcement directive make up the legislative framework for the protection of personal data in both the law enforcement context and, from the GDPR side, for consumers, citizens, donors and individuals who provide data – including to the third sector. The fundamental importance of all these measures is to increase the level of protection for citizens of the EU and of the UK. Bottom line, all these measures are intended to enhance the trust individuals have in the digital economy and in the effectiveness and

fairness of law enforcement. These measures, including the Privacy Shield and the umbrella agreement, go to the heart of the need to protect individuals, but also to facilitate and enable the flow of data for appropriate purposes, be they commercial, Government or law enforcement purposes.

In terms of the GDPR and the law enforcement directive, this is an evolution, not a revolution, of laws. We have had strong data protection laws in the UK, and still do. The General Data Protection Regulation and the law enforcement directive enhance that and bring a more 21st-century approach to the protections that individuals need, as we increasingly spend our lives online. In terms of the legislative instruments, that is the purpose. The benefit for business of the GDPR is a harmonised set of rules in the European Union. Business likes consistency and harmonisation. Citizens benefit because of the stronger controls.

At a high level, the Privacy Shield is really about a framework of assurance and a legally-binding arrangement to protect the flow of data from the EU to the US. The US has a set of measures to ensure the protection and oversight of those data flows. The same applies to the umbrella agreement, but in a law enforcement context it sets a harmonised and high level of protection from which other agreements can flow in a harmonised way. That is my short answer.

The Chairman: Could you explain to us your role in monitoring and enforcing the data protection standards in the UK and the EU, including with regard to EU agencies such as Europol?

Elizabeth Denham: First, I would stress that it is very important that the Information Commissioner is an independent regulator. I report to Parliament, not to the Government of the day, and I can give an independent adjudication, an independent decision or advice to Government and to Parliament.

Our work on the ground domestically runs the gamut from providing guidance, advice and good practice visits to UK organisations, right through to taking out the stick from the cupboard and enforcing the law, as we have done in many cases. Our role in European arrangements such as Europol, Eurojust and the Schengen information system is to contribute to the co-operative oversight of those arrangements and ensure that UK citizens' privacy rights and data protection rights are respected in those fora. We are very involved in audits, investigations, etcetera. We have a strong role there.

The Chairman: When we leave, what will the implications be for Europol and your monitoring role there?

Elizabeth Denham: If we leave Europol and the other arrangements and we become a third country, so we are not involved in them, the impact is that the ICO—the UK's regulator—will not have an oversight role when it

comes to investigating and reviewing the very sensitive data, (including UK citizens' data) , involved in those co-operative arrangements.

Q24 **Lord Cormack:** There was a reminder this morning, in the news from across the Atlantic, of what a vast job this is. How many people do you have to assist you? What is their level of qualification, and are you confident that you have enough?

Elizabeth Denham: Almost every regulator would say that he or she does not have sufficient resources. I have approximately 500 people to support me in my adjudicative and educative functions across the United Kingdom. With the coming of the General Data Protection Regulation, we will have more responsibilities and new enforcement powers. For example, when there is a security breach involving personal information, in many cases there will be a mandatory requirement for companies and public bodies to report to us.

We are putting in new measures to address our new regulatory powers. We have given Government the estimate that we will need, over the next two to three years, another 200 people to do that job. I have lawyers who work for me. I have investigators, former policemen, policy analysts and advisers who answer the phone, so a range of people. However, this is becoming a more complex area of law and regulation, and just trying to keep up with technology and the challenge of technology is difficult.

Lord Cormack: How many offices do you have around the country?

Elizabeth Denham: I have four offices. I have offices in Northern Ireland, Scotland, Wales and I have just opened a London office. However, the main part of my office, where 450 people are based, is in Cheshire, just south of Manchester, for historic reasons.

Lord Cormack: Is that where you operate from?

Elizabeth Denham: That is where I operate from, but I spend a lot of time in London.

Baroness Massey of Darwen: It sounds exciting.

Lord Cormack: It sounds overwhelming.

Baroness Massey of Darwen: I am sure she is not overwhelmed. Could you say what the education function is?

Elizabeth Denham: The education function is probably the most important function that we have, especially when you have a new Regulation coming in. This is a once-in-a-generation change in the law, and we are the primary educators: for data controllers on their new responsibilities; and for the public on their new rights.

On the GDPR, on Monday we held a conference for 800 data protection practitioners who gathered in Manchester. It was live-streamed to probably another 4,000 people. We give sessions and, most importantly,

we publish guidance to interpret the new law. Just last week, we issued draft guidance on the standards of consent under the new GDPR.

Baroness Massey of Darwen: How do you educate the public?

Elizabeth Denham: That is a challenging one. It is done through the media. We have quite a user-friendly website. We attend public interest conferences. We are very connected with civil society groups. That is a way to reach the public, but reaching the general public is challenging.

Lord Jay of Ewelme: Following up what you were saying about the meetings and the streaming that you have done, have you been focusing in your education function on the changes that Brexit is likely to bring to data control or just on what the position has been up until now? Are you changing day by day, as we get closer to leaving?

Elizabeth Denham: We have been focusing on educating data controllers and data processors on the changes that are coming in with the General Data Protection Regulation, because when the Regulation comes in, in May 2018, we will still be in the EU. It will be the law of the day. As a regulation, it is directly applicable. Even though we have to educate and to change our own functions, we still have to keep up with the day-to-day work of the office, which feels a lot like changing tyres on a moving car.

When it comes to what the regulatory environment will be post-exit, we do not know the answer, but we have a lot of work going on with our policy staff, so we can give advice to Government, Parliament and pretty much anyone who asks about what the various impacts of different arrangements would be post exiting the EU.

Q25 **Lord Watts:** Following the Chairman's question, assuming that the UK will be treated as a third country for data protection purposes once we leave the Union, what is the default position if we fail to secure an equivalence deal with our European partners? What would we do on day one?

Elizabeth Denham: I have said publicly and to the Government that, in my view, the best way forward is to achieve an adequacy finding from the European Commission. That is the best way forward because it is the most straightforward arrangement for the commercial sector and certainly for citizens and consumers who want their data transferred and interchanged between the EU and the UK. We want data flows to continue; it is the most straightforward process by which to achieve that.

Achieving adequacy on day one after exiting the EU may be challenging, because there is a legal process involved, which includes assessment and obtaining an opinion from the Article 29 working party, which is all my counterparts working together in the EU. It is up to Government to determine whether to pursue an adequacy finding. If there is a way to negotiate either a transition arrangement or something so that there is not a cliff edge on day one, that is in the best interests of everybody.

Lord Watts: We would all agree that the continuing flow of information and data is desirable, but what happens if that proves to be impossible? As the Commissioner responsible for the UK, how will you deal with a situation where you do not have an equivalent deal and you have no mechanisms to cope with the job that you have been set?

Elizabeth Denham: Again, it is not for me as the regulator to determine what the regulatory measures and environment will look like after exit. However, there are measures other than adequacy that allow data to continue flowing. In the General Data Protection Regulation, similar to the existing law today, companies can rely on standard contractual clauses, binding corporate rules and the consent of individuals. These are all legal measures to allow and provide for the transfer of data. They are just more difficult than having a comprehensive adequacy finding so that data can flow.

Lord Watts: Do you think there is a danger that the data flow may stop if that deal is not reached?

Elizabeth Denham: That is a theoretical question: will data stop? It is hard to imagine that data will stop because businesses will want to continue, but if there is no underlying legal authority for the transfer of data we will have issues of complaints, investigations and enforcements, including by the courts. If data flows, it may flow in contravention of European law and the Regulation.

Lord Watts: Potentially, as the commissioner, you have a responsibility to make sure that data is protected. If there was no deal in place and you could not satisfy yourself that that was the case, would you have to take legal action to prevent data being exchanged without the protection that you have a statutory obligation to make sure that it has?

Elizabeth Denham: I have a statutory obligation to enforce the law, and if data was flowing in contravention of the law and we received a complaint or were made aware of that, then yes, there would be onus on me to take action. I am very much hoping that we will not see that situation, because it is in the interests of everyone—as everyone in this room knows—that data continues to flow for appropriate purposes, within control and with protective measures for individuals.

Lord Jay of Ewelme: Following on from that, if on day one you have not had an adequacy decision agreed but you are in the process of doing so, are there various mechanisms to enable data to flow and you to continue your function within the law? Are they laid down somewhere or do you have to invent them with the Commission? What would happen between day one and day 300, let us say, if you were pretty confident that on day 300 you were going to have an adequacy decision?

Elizabeth Denham: If the Commission was assessing the UK's laws and enforcement of those laws (taken in the round, because that is what is needed for an adequacy decision or essential equivalency), there are

other mechanisms in the law that would allow it, but they are not as broad, all-encompassing and clear as an adequacy arrangement.

Lord Jay of Ewelme: The Commission would allow you to get through an interim period when you knew what you were going to end up with.

Elizabeth Denham: That is for negotiation between the UK Government and the European Commission, because it is the European Commission that grants an adequacy finding to a third country.

Lord Jay of Ewelme: If the decision were taken, for whatever reason, not to go for an adequacy finding, are there alternatives that are good, almost as good or would at least allow data to flow? What are the alternatives to an adequacy finding, if it is decided not to go for one?

Elizabeth Denham: There are only, I believe, nine jurisdictions¹ that have an adequacy finding, or at least a partial finding, by the Commission. Canada is one of those jurisdictions, Canada's is a partial adequacy finding just for the commercial sector. There are other ways for data to flow. There are other types of agreements that could be put in place, but they are not as straightforward. It is certainly not as easy for businesses, particularly small and medium-sized businesses, to negotiate binding corporate rules and standard contractual clauses.

I would like to make one more point about that. Comparing the UK to other countries that do not have adequacy is missing a major point. There is no comparator to the UK. The UK has been so heavily integrated in the EU that it is difficult to say that the UK can get by without an adequacy arrangement and be just like—you can pick a country—Turkey or Brazil. It is just not the same.

Lord Jay of Ewelme: Is that an incentive for the UK and the Commission to come up with a solution, simply because it would be unthinkable not to, given the degree of data that is flowing between the two as a result of 40-year membership of the EU?

Elizabeth Denham: It is up to Government and the Commission to negotiate what that would look like. I am an expert adviser to them. I am certainly a long way from the negotiating table, but according to my staff and from my own experience internationally—because I have been very involved with the privacy authorities in the Asia-Pacific region, so I know the situation of Singapore, Japan and South Korea well—none of these countries have an adequacy finding, and data flows with other types of protections.

However, my point is that the UK is pretty special, because of the level of integration we have had with the EU and our role in devising and developing the General Data Protection Regulation and the law enforcement directive. We have been front and centre in this work, and

¹ Actually 12. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

we have a lot to be proud of in our contributions to the protection of personal data.

Q26 Lord Cormack: You said something a couple of minutes ago that rather alarmed me. You said you were a long way from the negotiating table. Of course, I understand that, but are you confident that your enormous experience and your responsibilities mean that Ministers and those who are negotiating are talking sufficiently with you?

Elizabeth Denham: I have been advising. I have provided papers and been in discussion with Ministers and senior government staff. We have seconded some of our staff from the ICO into Government, , because of their long experience, to assist with the policy analysis that the Government is undertaking. The Ministers' doors are open and we are actively providing advice.

Lord Cormack: That is comforting. It is not quite the job you applied for, though, is it?

Elizabeth Denham: It is really interesting.

Lord Cormack: I am sure it is, and that covers a multitude of sins.

Elizabeth Denham: I have long admired the UK's system, UK law and the ICO as a very progressive, tech-savvy organisation and a pragmatic, practical regulator. I am pleased to be able to contribute to that.

One of the points that I have brought up with Government and want to emphasise to this Committee is that it is very important that the Government consider the ICO's place and its influence in what is going to be the European Data Protection Board. The Government should do what they can to ensure we have some status, be it observer status or something that looks close to "close", as opposed to being a third country.

The European Data Protection Board is going to be an adjudicative board; it will not just be an advisory board, as it is now. The European Data Protection Board will make decisions about the data processing of companies and organisations that impact on UK citizens. If the ICO, as the UK's regulator, is nowhere close to those decisions, it will be frustrating for citizens, for UK business, and for Government.

Lord Cormack: I hope we will be able to make recommendations along those lines.

Lord Condon: Is the data protection board staffed and run by politicians, or are information experts making those decisions.

Elizabeth Denham: The European Data Protection Board will be composed of independent data protection authorities across the EU 27. It will be supported by a secretariat. My counterparts will be sitting at the table and making a joint decision about (for example) whether Google's new policy on X, Y and Z is appropriate for the European Union.

Q27 **Lord O'Neill of Clackmannan:** In some respects, you have answered part of this question. On the role of the board, would it ultimately end up at the ECJ?

Elizabeth Denham: Yes.

Lord O'Neill of Clackmannan: That is anathema to number of the Brexiteers: anything that is sullied by a close proximity to the ECJ is unacceptable, so I will just lay down that caveat. Have you given wider consideration to your role and functions, post Brexit, given the options that are available? It is heartening to know that you are advising Government about the nitty-gritty of the negotiation. Beyond the horizon, have you been doing any thinking on that?

Elizabeth Denham: I have been doing a lot of thinking about the role of the ICO internationally. There has been much focus over the last four or five years, in the development of the law enforcement directive and the General Data Protection Regulation, on Europe. The ICO is one of the largest data protection regulators globally. We have 35 years of experience in this space and we now have a new international strategy, which has been developed in the last few months. In this strategy, we will continue to lean in and engage deeply with the work of our European colleagues on the implementation of the GDPR. We are front and centre, doing a lot of work there.

At the same time, we are engaging in global enforcement work beyond Europe, to build bridges with other regulators around the world. I had a meeting with the new Japanese Personal Information Protection Commission, and we are setting up a memorandum of understanding for co-operative work. I will be going to the US to build bridges with the Federal Trade Commission, which is partially my counterpart there. We went to a meeting of the Asia Pacific Privacy Authorities in December, so a lot of our work is going to be beyond Europe, not just because of exiting the EU but because data knows no borders. We need to work together. All data protection standards are being raised across the globe.

Lord O'Neill of Clackmannan: Would these bilateral deals take effect after Brexit or would they be in place beforehand? A number of the international agreements in which Britain is currently placed because of our membership of the EU effectively preclude us from entering into formal arrangements prior to a date of departure. Are you saying that, in your area, you have a greater degree of flexibility?

Elizabeth Denham: I do, because if there is an investigation or a data breach that involves several jurisdictions, I now have the ability to enter into agreements with other jurisdictions to co-operate and enforce the data protection law.

Lord O'Neill of Clackmannan: That is regardless of the consequences for the EU.

Elizabeth Denham: Yes. I could work with Canada, Australia, US, et cetera.

Lord O'Neill of Clackmannan: You deftly sidestepped the question about whether you have adequate resources to do what you are doing. Have you made an assessment of the resource requirements approaching the post-Brexit situation? You seem to have a very ambitious programme, which will require a lot of bodies and a lot of travelling, from what you are saying, as well as just working in the UK. What thought have you given to the resource implications of the impending departure from the EU?

Elizabeth Denham: We have assessed our need for increased resources—technical, staffing and physical space—in the next three years. Because the GDPR is coming in regardless of exiting, we knew that we were going to need new resources, so we have done a business case and have put it before Government. I know the level of resources we need to do the job. What the environment looks like in 2019 or 2020 I cannot say precisely at this time. However, we know that even if we were staying in the EU, our international work would be increasingly important and these other jurisdictions would impact on the UK. Decisions that are made in Singapore about data protection will impact here. Courts are looking at each other's decisions. It is a global world when it comes to data.

Lord O'Neill of Clackmannan: In the eight months you have been in the job, have you had support from embassies in capital cities such as Tokyo? Do you feel you are on the same footing as the embassies, so that they are able to give you assistance and support?

Elizabeth Denham: I feel supported. It is working well and I feel supported.

Q28 **Lord Soley:** We have been told on a previous occasion that we set a high standard in the UK for data protection, and everything you have said confirms that. Given the movement worldwide and between the UK and the EU, is the logical way forward for the UK to endeavour to set the gold standard in data protection, so that we could have what would be equivalence not only with the EU, but with other countries around the world? Is that not the way forward? That way, we are seen as the country you come to to get the best standards, and therefore you can exchange data with us. Is that right?

Elizabeth Denham: That is absolutely right. If we want to innovate with data—not just in the private sector but in the public sector—use data for effective public policy reasons, we have to have a high level of trust from individuals, which means that we need the gold standard of data protection regulation and enforcement. They go hand in hand. The right way forward, from my perspective, is to fully adopt the General Data Protection Regulation and put the law enforcement directive into effect.

This is very important: the best way forward is a unified implementation of those instruments, because we have to build that level of trust. We cannot have people throwing rocks at us from the outside. We have to have a very strong regime here, enforced well. Weakening the law and

reducing the so-called burden on business may seem attractive when you look at it on the surface, but a lowering of data protection regulation and practice would not be a sustainable business model. That would really bite us in the long-term.

Lord Soley: Contrary to that, would Singapore and Japan already look to Britain as a sort of gold standard?

Elizabeth Denham: They are looking to Britain and the ICO already because of our extensive pragmatic guidance, written in English, which is helpful for them in their newer regimes. I spent quite a bit of time with the Singaporean Government in the development of their law when I was working in Canada. It looks like Canada's law, but it is getting stronger, to keep up with the GDPR.

Q29 **Baroness Massey of Darwen:** I want to ask you two questions, and you have alluded to certain aspects of both, but I want to focus down a bit. First, what are the main channels through which the UK can influence global data protection standards and how much influence do we actually have? Will that change post Brexit?

Elizabeth Denham: I have already spoken about the European Data Protection Board. It is critical that we have some kind of influence there. I see, as I sit around the table at the Article 29 working party, Norway as an observer, but it does not sit in the background. Norway is involved in, or even a rapporteur for, some of the work, so the EDPB is an important arena. So is the International Conference of Data Protection and Privacy Commissioners, where all the data protection commissioners globally work together.

Baroness Massey of Darwen: Is that a regular meeting place?

Elizabeth Denham: One hundred plus data protection authorities around the world participate in a conference every year, and work goes on between the conferences. My office is chairing a piece of work to enhance global co-operation: a framework for global enforcement. That is a really important forum. The Asia Pacific Privacy Authorities that I have mentioned are very important. We are co-chair of a group of Commonwealth countries called the Common Thread Network. We are working within the Commonwealth to help raise the bar for some countries that do not have strong data protection laws and to work on consistency across the board.

The end game, five or 10 years from now, should be an international treaty on data protection. Right now, we have a patchwork. Some jurisdictions seek to apply to Europe for an adequacy finding. One jurisdiction questioning another country's equivalency. A global treaty is on the horizon, but that is where we need to go if we recognise the global nature of data flows.

Baroness Massey of Darwen: Do you think that will change for the UK, post Brexit?

Elizabeth Denham: No, I think we will be involved in all those fora. The one I am worried about is the European Data Protection Board. It will be very influential.

Baroness Massey of Darwen: When will the framework that you mentioned be ready?

Elizabeth Denham: The framework for the European Data Protection Board will be in place in May 2018. My counterparts in the Article 29 working party will shift from an advisory body to the Commission, to an adjudicative body that will make decisions about cases and have a consistency mechanism for determinations made across Europe on data protection. If we are outside the EDPB, pressing our faces on the glass, the UK will be without influence and yet have adopted fulsomely the General Data Protection Regulation.

Baroness Massey of Darwen: Is there any sense of what will actually be in that framework? It sounds very interesting.

Elizabeth Denham: Yes. A lot of work has been done, and, if I may, I could follow up with the Committee to outline how the board is going to work and what the framework will look like.

The Chairman: That would be very helpful.

Baroness Massey of Darwen: My second question, which you have also touched on before, is this: what is your assessment of how much room for manoeuvre the UK Government will have on data protection policy post Brexit, if they want to maintain unhindered flows of data with both the EU and the US?

Elizabeth Denham: If the Government decides to proceed and obtain an adequacy finding for the UK as a third country, that will limit how much manoeuvre we have. We will have to keep our laws up to an equivalent standard, which will be assessed every three or four years. There will be some constraints around that. That said, the GDPR itself has a lot of white space in it. There is still a lot of room for manoeuvre so that domestic authorities can carve out and make the laws they want.

I am going to give you some examples. Decisions can be made at a domestic level on children and age of consent and on balancing freedom of expression and the role of media with data protection. Those are examples of where the GDPR is not so prescriptive, so the UK would have room. However, when you bind yourself to an adequacy decision, the European Commission will put constraints in place. The Privacy Shield is a EU-US agreement, and if we are a third country we will not be part of it, so we will need to strike our own agreement with the US.

Lord Cormack: You talked about the need for international agreement some years down the line, and that is clearly very important. You talked about 100 countries working in co-operation. I have two questions. First, are all the present members of the EU effectively operating? Secondly, which major countries are not co-operating?

Elizabeth Denham: Are you focusing on the EU or on the 100 countries?

Lord Cormack: First, are you satisfied that all the EU countries have a high level of competence in this regard? Secondly, are there any major countries that are not within the 100 to which you refer?

Elizabeth Denham: I have not done an assessment of the effectiveness of the regulation across Europe, so I could not speak to that. Country by country, the laws are different; some regulators are better resourced than others, some have different priorities. It is a very challenging question. I have worked for 20 years in the data protection space and a dozen years as a regulator, and there is now a great desire for more harmonisation and higher standards. Across the globe, there are more laws, the laws look as though they are converging more than they did in the past, and the independence of the regulators is becoming a really important component of that. The forums are active. There is much work going on. There is much collaboration, which is very positive.

That demonstrates that data underpins and runs through all our human activities. That is why data protection is not a back-room, back-office, backburner issue any more. It is front and centre and integral in the societal debates that we are having right now.

Lord Cormack: Of the 100 countries, are there notable exceptions? Is Russia one of the 100 countries?

Elizabeth Denham: Russia is not an accredited member of the 100 plus jurisdictions sitting at the table.. I know that China is working on a commercial data protection law. Singapore has a commercial law. The membership has doubled in the last four or five years. You can see that countries are interested in passing these laws, but the question about whether they are effectively regulated is a really good topic for an academic study.

Lord O'Neill of Clackmannan: I just want to clear up something that I was not very sure about. You said that Norway, as a thirdparty, had an influential role by sitting on the Committee and actively participating. Which Committee was that? Was it the Committee that would ultimately have the adequacy decisions flowing from it?

Elizabeth Denham: No. Norway, as a member of the EEA, has observer status in what is now the working group of data protection authorities across Europe – the Article 29 Working Party. Norway has a way in, with observer status, but it is an active member. It attends many of the meetings. It even leads some of the work. If the UK was outside the EEA, it would be a third country. Our participation in that forum would need to be negotiated between the Government of the UK and the European Commission, because the European Commission really runs that.

Q30 **Lord Condon:** When this Committee looked at police and security co-operation post Brexit, it was suggested to us that the UK has been very influential and has been a moderator in helping to set the balance

between security needs and privacy. There was almost a warning that when we leave the EU will shift more rapidly towards privacy requirements—perhaps, some would say, at the expense of security requirements. Is that a valid observation or a valid fear about how the EU might shift the balance in the absence of the UK's influence?

Elizabeth Denham: I cannot speak to the involvement of the UK in the actual operations of these various co-operative endeavours in police and criminal justice, but I have heard that observation. I do not know if it is true, but the ICO and the UK have been very influential in making the point that it is not public safety or privacy; it is public safety and privacy. This is not a zero-sum game. It is really important that we stand for that message. In my five years as commissioner, I am going to live and breathe the message that one should not come at the expense of another.

That said, this is a really difficult and challenging balance to make right now, with all the threats in the world. The tilt towards privacy over public safety or privacy over law enforcement, again, is difficult; it is challenging. The courts are getting involved in it more and more, and that is something that Governments cannot completely control. It is up to the courts to do some of that balancing.

Lord Condon: Linked to that, can you help us understand how, say, the latest law enforcement directive and/or the EU-US umbrella agreement deal with national security exemptions? Are they written into those directives and agreements? How does your office police the boundaries of that? Are you comfortable with the way it is done?

Elizabeth Denham: I will start with the legal instruments: the law enforcement directive and the umbrella agreement. The law enforcement directive codifies the practices, and gets the balance right with the exemptions for law enforcement and national security, so, on a legal basis, yes. The umbrella agreement is really a high-level set of principles that tries to create a level playing field for all the agreements and activities that come under it. The umbrella agreement between the US and the EU tries to raise the standard of protection but to allow and facilitate appropriate data flows.

Lord Condon: Are you comfortable with the role your office has in policing the boundaries?

Elizabeth Denham: We have a very limited role in policing national security. That will be primarily the role of the new commissioner under the Investigatory Powers Act. We have a very limited role in that. We have an oversight role in the co-operation initiatives such as Eurojust and Europol, so we have a role in policing how sensitive information is being collected, used and disposed of. I am satisfied with that. Will it continue? I do not know.

Q31 **Lord Jay of Ewelme:** We talked a bit about what may happen after Brexit. I wanted to come back to what you were talking about at the

beginning, the General Data Protection Regulation and the law enforcement directive, which will have legal effect, as I understand it, from May of next year. The Government will have to produce an impact assessment of the impact of the various directives and regulations. I wondered whether you could say anything about your assessment at the moment of the resource implications for businesses and other data controllers of complying with both the General Data Protection Regulation and the law enforcement directive.

Elizabeth Denham: The impact on businesses depends on how much work they have done to comply with the current regime. We have had the Data Protection Act in the UK since 1998. As I said, the GDPR has higher standards, but they are evolved standards. If a company has not been doing anything for the last 10 years on data protection, yes, the resource implications are going to be larger.

My observation since I have arrived in the UK, though, having spent a lot of time with industry groups and other commercial groups, talking to tech innovators -- is that they now see the value in strong protection for their consumers and that it equals good business practice. In other words, it is a competitive advantage if you are doing the right thing with customers' data. Playing fast and loose with individuals' sensitive personal data is not going to cut it. There is an impact. It is greater on companies that have not done much to comply in the past. There are lots of tools out there to help them.

Lord Jay of Ewelme: Does it tend to be the larger companies that have tried to cope with the burden, and the smaller and medium-sized enterprises that have not, or does that not necessarily apply?

Elizabeth Denham: The small and medium-sized organisations are the sector that keeps me up at night when I wonder how we can help them. We have developed toolkits. We have developed special checklists. We have focused some of our education on small and medium sized firms.

The other way I am trying to do it is by reaching out to other groups that have a direct link to small businesses. I spoke to the Institute of Chartered Accountants in England and Wales, because its clients are small businesses, so there is a way for us to have a cascading effect to small business. It is important, with the number of small businesses in the UK, that we do what we can to give online tools, education seminars and special guidance, such as, "The top 10 things you need to do for the GDPR".

Q32 **Lord Soley:** You gave the example, in your lecture to the accountants, of Facebook taking over WhatsApp. When that happens, if I have given my name, address and contact details to WhatsApp, presumably they automatically go to Facebook, which then has access to them. That is presumably governed in some way by your messages to them, but there must be umpteen small companies that get merged up in that, where that information is taken over. I simply observe from my own life, as others must, that adverts suddenly appear on your various channels, and

it is clear that that information is not being protected in some way because they have access to it. How do you address that with the umpteen smaller companies? You mentioned a bit of it, but is that not a really big problem?

Elizabeth Denham: It is a really big problem. In investigating and focusing on Facebook-WhatsApp, we are looking at how Facebook and WhatsApp can be more transparent and give persistent opt-outs to consumers so that the information does not flow. That is the focus of our work there. It is an ongoing file, so I cannot say much about it. In the background, we have started another piece of work, which is about mergers and acquisitions. When two companies merge with the purpose of the merger being greater access to consumer data, we need special rules around that for individuals. Promises and commitments made in one company should be persistent and should flow with the data.

Lord Soley: Specifically on that, if someone ticks the box that says, "Do not send me any more garbage on this, over and above what I have asked you to do", does that automatically carry over and, if it does not, is that an offence?

Elizabeth Denham: That could be an offence under PECR, but I would have to look at the specifics of it. If it is helpful, I can write to you with some examples of where we have looked at precisely this issue.

Lord Soley: That would be helpful, because there must be many examples like that, judging by what happens to my information one way or other.

Elizabeth Denham: There are many examples.

Q33 **Baroness Browning:** In the context of what you have been telling us about companies, could you say a few words about data held by the public sector, including arm's-length government agencies? I have to say I would be more concerned about what the Driver and Vehicle Licensing Agency is doing with my data than certain companies I buy things from online. What is the situation with public sector data, and how does it compare with other countries?

Elizabeth Denham: The rules are the same. The rules in the Data Protection Act apply to commercial actors, the third sector and the government sector, including arm's-length bodies. The focus of a lot of our work has been on the public sector, particularly around significant data breaches where data is lost. We have also had many investigations that I think assist public bodies in the proper use, collection, disposal and retention of personal data. The rules are the same. Is your question whether the UK public bodies are caring for data in a respectful way, comparatively?

Baroness Browning: Yes.

Elizabeth Denham: The public sector knows what the rules are. It tries to comply. The resources are scarce in the public sector.

Baroness Browning: That is no excuse, though, is it?

Elizabeth Denham: It is not an excuse, but having the resources to do the work is a challenge for public bodies. I was really encouraged by how many of the public sector data protection practitioners who attended our conference on Monday in Manchester have formed networks to share best practices to ensure that every public body does not reinvent the wheel in its governance structures, et cetera. Some people are more worried about the public sector; some are more worried about the private sector. We cover both.

Q34 **Baroness Janke:** We heard last week that there appear to be quite a few areas of non-compliance, and I am a bit alarmed by this. I was just wondering how big a problem you see it to be. As far as members of the public and your role of protection are concerned, I am not aware of a great deal of public awareness as to how they are being protected in this way. That is the first part. The second part is in relation to the EU and the adequacy decision. Is the level of non-compliance an obstacle in that?

Elizabeth Denham: I am going to start with the second part of your question first, if that is okay. The level of compliance within a third country is not a criterion for making an adequacy finding. There are specific criteria in the GDPR, which I could share with you, which are the ones that the Commission will look at. I also want to emphasise that adequacy does not mean exactly the same; it does not mean a carbon copy. It means essential equivalence, and the Commission will look at that in the round. Whether there are many non-compliant companies in the UK will not be an issue; the effectiveness of the regulator will be. Again, what is the independence of the regulator? Is there an effective regulator doing an effective job? Those will be part of the adequacy determination.

In terms of my assessment on non-compliance, which was your first question, if we had total compliance I would not have to get the stick out of the cupboard and use my enforcement powers, but I do not know any country where you would find completely compliant companies and public bodies, especially when we have many small companies innovating with potentially large amounts of sensitive personal information. It might be two people working in their garage. This is a new phenomenon.

I see examples of very small companies that have high compliance, and examples of larger companies or public bodies that are perfectly compliant across the board. We are looking at this every day. I can give you a report on how many enforcement actions we have taken and in what sectors.

Baroness Janke: We heard last week that the number was high with regard to judgment for adequacy. As we move on to more and more sophisticated sharing of information, I am not suggesting that it is realistic to expect every single firm to have a high level of compliance, but one of the people who gave evidence last week gave the impression that there are pools of data out there in companies. Baroness Browning

has mentioned public authorities. Are the public aware of this? My concern is that we have talked a lot about helping companies and enabling the flow of information. You have satisfied us that it is not a problem as far as adequacy is concerned. I would like to hear a little more about how the public are protected and how proactively you are pursuing that particular objective.

Elizabeth Denham: It is a big challenge. The public cares more about their rights than they have in the past, which may be partially because so much of our life is lived online. We suffer cyber-attacks and lose our data. We suffer ransomware. We get marketing without understanding why it has been directed to us. We are all on the front page on this, but on the other hand my job as a regulator is to pull back the curtain to show the public what is actually happening with the processing of their data. It is very opaque to the public. They do not understand the chain of companies that is involved in a single transaction.

The work that I am doing with WhatsApp and Facebook will pull back the curtain on that. It will help to educate the public. We are now starting to look at the use of sophisticated analytics and the targeting of messages, even in the political realm. The public need to know about that too. A really important part of the work that we do is revealing to the public how data is processed, shared, traded and advanced. Do the public know they have rights around this? We are doing what we can.

Q35 **Lord Soley:** Are there any infraction proceedings against the United Kingdom at the moment involving implementation of the 1998 Data Protection Act? Are any proceedings under way or in the pipeline?

Elizabeth Denham: Do you mean infraction proceedings between the UK and the Commission?

Lord Soley: Yes.

Elizabeth Denham: There is a freedom of information request and adjudication going on right now, in which an individual is attempting to get access to information about infraction proceedings. I cannot speak to the details of that; I am not a party to the infractions proceeding, but that is a legitimate question that this Committee could ask Government, as Government are a party to that. As a third party to those proceedings, I do not have that information.

Lord Soley: It is between the European Commission and the Government, and you do not have any involvement in it at all.

Elizabeth Denham: I do not, except —

Lord Soley: You know about it.

Elizabeth Denham: I know about it because I received a note just yesterday, in preparation for these proceedings I know there was a freedom of information request to get access to the information about the infraction proceedings, but it has gone to the tribunal, which is away from

my remit. The best way to get access to that information would be through the Government or the Commission.

Lord Soley: You are aware of only the one example that has come across your desk because of the Freedom of Information Act. There is nothing else that you are aware of.

Elizabeth Denham: There is nothing else that I am aware of².

Lord Soley: To some extent you have hinted at the way forward on this, but I want to know how you feel that once we leave the EU the Privacy Shield could work with the United States. Could we have something modelled on the Swiss example for the EU-US Privacy Shield? Should we, as you indicated in an answer to me earlier, just try to set the gold standard? Do we pick up a model like the Swiss one, in that example, or try to develop something ourselves?

Elizabeth Denham: If we are a third country, we will have to strike some kind of arrangement between the UK and the US, to protect those data flows. That is what UK citizens would expect and what the law is going to require. I do not see why we need to completely reinvent the wheel. Looking at the existing Privacy Shield and the Swiss example that has just been struck would be a starting point. I go back to my earlier point that the UK is in a special situation because of the integration of everything that we have done in the last 40 years with the EU.

Am I saying it is a bespoke arrangement? These agreements are a starting point. Why would we start with a blank sheet of paper? We would look at them and see if we need to make some changes or adjustments for our own situation.

Lord Soley: Presumably, because we are to some extent a country setting the standard, the US might want to be very close to us on this. Is that right?

Elizabeth Denham: It might.

Lord Soley: We do not know.

Elizabeth Denham: We do not know.

Lord Soley: Can you tell me how important the Privacy Shield is to the UK economy? Do we know how many and what types of UK-based companies rely on it?

Elizabeth Denham: The ICO does not record the number or types of UK data controllers who transfer data to Privacy Shield members in the US. We do not have a register of which companies are using it. That said, we know that 1,800 US companies have certified to the shield, and there are many, many more in the pipeline. I also hear, especially from small and

² Note – in the past the ICO has offered advice to the Government in connection with infraction proceedings concerning data protection matters.

medium-sized business, that this is the preferred fundamental mechanism for transferring data, because it is broader and more comprehensive than the standard contractual clauses, as we talked about. There were more companies signed up to Safe Harbor, but you have to give the Privacy Shields some time. The bottom line is that it is important and helpful to businesses to have a shield or a similar arrangement in the future.

The Chairman: How interested do you think the USA will be in striking a Privacy Shield type of agreement with the UK?

Elizabeth Denham: I do not know. I do not have the answer to that. We are a strong and important trading partner, but that is theoretical. I am not sure I have any evidence.

Q36 **Lord Condon:** Could we go back to the EU-US umbrella agreement, the high-level framework for law enforcement co-operation? When we leave the EU, do you think there is a need and would it be sensible to seek to negotiate an equivalent umbrella agreement, UK to EU and UK to US? Presumably at the point of Brexit we should be pretty well harmonised, but in order to secure the future do you think it is realistic that we should seek to enter into those sorts of agreements with the US and the EU?

Elizabeth Denham: Any arrangement that gives us a strong, harmonised approach for protection of personal data and facilitates the appropriate transfer of data is a good thing. Rather than a series of bilateral agreements with independent member states of the EU, an umbrella agreement would be helpful. Harmonising the data protection rules for the law enforcement sector, including the rules about transferring personal data for criminal justice and law enforcement, and having cross-border co-operation, is a fundamentally important area for the public. I would expect the public to want us to all get on with this and make sure the data is protected, but also that there is facilitation of the appropriate transfer.

Lord Condon: You think the umbrella agreement between the EU and the US is a reasonable starting-point model to look at.

Elizabeth Denham: It is, but, as you said earlier, at the time of exiting the EU, we will have implemented the law enforcement directive. That will be really helpful, but the law enforcement directive has to be implemented in a unified fashion, not through a fragmented "Swiss cheese" approach. That is really important.

Baroness Browning: Given the relationship between the US and Canada, your experience in Canada, and of course the very long border between the two countries, how harmonised is the umbrella agreement between Canada and the USA?

Elizabeth Denham: On the umbrella agreement between Canada and the US, and the collaboration and co-operation for law enforcement, they share a heavily accessed border and there are information sharing arrangements and agreements. Interestingly, though, data protection

culture and practice is quite different, but when it comes to border security there is much work towards a harmonised agreement.

Q37 Baroness Browning: Looking, post Brexit, at the UK and its relationship with the EU, would that be a model to work on? Although we are an island, we are not that far from France and there will be, in Ireland, a border between the EU and the UK of some sort. Is there anything from the model that has been negotiated between America and Canada that would be helpful in the sort of agreement we would want to see between the UK and the EU?

Elizabeth Denham: I need to spend some time on that. Could I come back to the Committee with a response to that question?

Baroness Browning: Yes, of course. Do you see any grounds for concern that domestic legislation could impact on the UK's ability to continue sharing data with the EU, post Brexit? There are court cases under way at the moment and I am not asking you to second-guess what the outcome of those judgments will be, but there are, for example, challenges to the Investigatory Powers Act and so on. Is that likely to destabilise the agreement that we are eventually looking for?

Elizabeth Denham: As you say, it is a bit too early to say, because we are waiting, for example, on the Court of Appeal decision in Tele2 and Watson. That will be telling, and it will be important for us to take into account for our domestic law. From recent CJEU judgments, it seems likely that the UK's surveillance and data retention regime would be at risk for a positive adequacy finding. You have heard that from others, so it is an area of tension and one that we need to focus on if the Government are going to move towards an adequacy decision. It will also inform the future relationships between the UK and the EU on co-operative law enforcement. It is important.

Baroness Browning: In the balance that you have described today in looking at this area of legislation, when you sit round the table with other EU representatives concerned about this, is there any recognition of the fact that the UK as a country has been subject to terrorist attacks for decades; that current threats are worldwide, particularly in mainland Europe more latterly; that this is a global problem, not just one for the UK; and that the UK introduced certain pieces of legislation on the back of really quite hard learned experience?

Elizabeth Denham: I can speak for my data protection colleagues around the table. I cannot speak to what the Governments of those Member States think. Among my colleagues around the table, there is a deep recognition, especially with the attacks in Nice, Brussels and Germany last year, that there is a global problem. You will have seen changes to domestic legislation in some of those countries. Again, it is a question of finding the balance. The tension is there. I am hoping it is resolvable. My colleagues recognise that, but when it comes down to the Governments and the decision-makers in Parliaments, I cannot speak to that.

Q38 Lord Watts: Sorry to take you back to an earlier question that you have already answered. I am conscious that you estimated you would need 200 new staff to deal with the problems and challenges that we face. Are you preparing for that now? Are you recruiting those 200 staff? Have they been agreed in post? It seems to me that you would not be able to get the specialist staff that you require overnight. It would take a period of time for you to recruit them.

Elizabeth Denham: The recruitment of the additional staff would take place over perhaps a three-year period. The staff needs are in relation to the new General Data Protection Regulation, new powers under PECR, and the expansion of our remit, new enforcement powers and the extra education that we will need to do. You are right: I cannot hire them overnight. This is going to take a lot of time. The specialist staff we need are especially hard to recruit, and I find that public bodies and private sector organisations are nicking my staff already. I have said, "Please leave the regulator alone, because the regulator needs the staff". Commercial entities can pay more money than government. We are doing socially relevant work and I want to keep my staff.

Lord Watts: Are you confident that you will be able to recruit them, given the challenges of not only recruiting the skills required but keeping the staff you have, when there will be demand from the private sector, which normally can outbid any public sector organisation?

Elizabeth Denham: It is a challenge. We need to be strategic in what we are offering. We will never be able to match the salaries, but we can offer other benefits, such as flexible working. We have all kinds of challenges in retention and recruitment. I have a plan, which I could share with you, but the recruitment will take a good deal of time.

Lord Condon: Have you secured the budget commitments to enable you to recruit the staff?

Elizabeth Denham: Right now, the ICO is mainly funded by notification fees. I do not know if this Committee is aware of that. Data controllers must pay a fee to the ICO to register their data processing. There is no notification system under the GDPR so the UK will need to come up with a new fee structure to fund the regulator. The Government has done a lot of work on this, in partnership with the ICO. We have a way forward, but it has to be approved by Parliament. Our new fee structure needs to be approved by Parliament, hopefully before 2018, when our notification fees fall off a cliff and we no longer have £22 million in funding.

Q39 Lord Cormack: You have an enormous task and you have been extremely helpful in sharing some of your thoughts with us today. How far will the lead-up to Brexit, and the attempt to replicate the sort of co-operative arrangements we currently enjoy, dominate or distort your agenda over the next three or four years?

Elizabeth Denham: When I took the job before the referendum, I expected that my job would primarily be bringing in the new GDPR and the law enforcement directive, being a member of EDPB and doing that

good work. I suspect, without being able to put a precise number on it, probably one-third of my time has been spent on policy issues, getting my head around this whole space and meeting with officials. We have had a lot of meetings with stakeholders, be they TechUK, civil society groups or the health sector, which is very concerned about the continued use of data for research. I have many meetings with stakeholders. Added to making sure the Government have the policy advice that they need and supporting Parliament in the same way, it takes up probably one-third of my time and that of my specialist policy staff.

Lord Cormack: Thank you very much, and good luck.

- Q40 **Lord Soley:** I am not sure you will know the answer to this. Before or after Brexit, you have described very vividly the problem you have in conveying to the population generally when their data is being moved around between organisations. Given that there are a number of software programs that warn you about viruses, why is there not a software program to warn you when a company that holds your data is being taken over? Do you know if any work is being done on that? That will continue to apply right across the world, not just in relation to Europe.

Elizabeth Denham: I am really glad you asked that question, because there are innovative uses of technology to help in “privacy by design” solutions such as the one you just mentioned. One of the announcements that I made on Monday is that we are initiating a research grants and contributions programme to support independent research and open source solutions of exactly that kind. In other words, what technology solutions could help consumers understand the risks and take control of their data? There is a lot of work being done in the UK. We are a leader in that in many universities. The ICO will be establishing a grants programme to do exactly that.

Lord Soley: I will give them some evidence.

- Q41 **The Chairman:** What would the practical impact be, were the UK to receive only a partial adequacy finding from the Commission after leaving the European Union?

Elizabeth Denham: We know that there are partial adequacy findings in other countries. Again, the best way forward is to have a unified, harmonised approach across all sectors. Partial adequacy is better than no adequacy, but I would be more assertive in proceeding with the full adequacy finding.

The Chairman: Can I thank you very much indeed for your very comprehensive answers? We wish you all the best for the future.