

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT

Seventh Delegated Legislation Committee

DRAFT DATA PROTECTION PRIVACY
AND ELECTRONIC COMMUNICATIONS
(AMENDMENT ETC.) (EU EXIT)
REGULATIONS 2020

Wednesday 25 November 2020

No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor’s Room, House of Commons,

not later than

Sunday 29 November 2020

© Parliamentary Copyright House of Commons 2020

This publication may be reproduced under the terms of the Open Parliament licence, which is published at www.parliament.uk/site-information/copyright/.

The Committee consisted of the following Members:

Chair: STEVE McCABE

Byrne, Ian (<i>Liverpool, West Derby</i>) (Lab)	† Mayhew, Jerome (<i>Broadland</i>) (Con)
† Caulfield, Maria (<i>Lewes</i>) (Con)	† O'Brien, Neil (<i>Harborough</i>) (Con)
† Clark, Feryal (<i>Enfield North</i>) (Lab)	† Onwurah, Chi (<i>Newcastle upon Tyne Central</i>) (Lab)
Cooper, Rosie (<i>West Lancashire</i>) (Lab)	† Roberts, Rob (<i>Delyn</i>) (Con)
Cryer, John (<i>Leyton and Wanstead</i>) (Lab)	Thompson, Owen (<i>Midlothian</i>) (SNP)
Cummins, Judith (<i>Bradford South</i>) (Lab)	† Whittingdale, Mr John (<i>Minister for Media and Data</i>)
† Fletcher, Mark (<i>Bolsover</i>) (Con)	
† Holmes, Paul (<i>Eastleigh</i>) (Con)	Yohanna Sallberg, <i>Committee Clerk</i>
† Howell, Paul (<i>Sedgefield</i>) (Con)	
† Hunt, Jane (<i>Loughborough</i>) (Con)	
† Hunt, Tom (<i>Ipswich</i>) (Con)	† attended the Committee

Seventh Delegated Legislation Committee

Wednesday 25 November 2020

[STEVE McCABE *in the Chair*]

DRAFT DATA PROTECTION PRIVACY AND ELECTRONIC COMMUNICATIONS (AMENDMENTS ETC.) (EU EXIT) REGULATIONS 2020

2.30 pm

The Chair: Before we begin, I must remind Members about the social distancing rules, as we are in a very small room. I see that Chi Onwurah has done her best, by limiting the numbers on the Opposition side to make it easier. [*Interruption.*] I also remind Members that if they have any speaking notes, our *Hansard* colleagues would like them at hochansardnotes@parliament.uk.

The Minister for Media and Data (Mr John Whittingdale): I beg to move,

That the Ctee has considered the draft Data Protection Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020.

It is a pleasure to serve under your chairmanship this afternoon, Mr McCabe. The statutory instrument was laid before both Houses on 14 October and is made under the European Union (Withdrawal) Act 2018. The main intention is to ensure that the UK's data protection framework will function correctly at the end of the transition period, and that there will be no data cliff edges. I want to bring to the Committee's attention the fact that neither the Joint Committee on Statutory Instruments nor the House of Lords Secondary Legislation Scrutiny Committee has drawn either House's attention to the SI.

Where the transition period comes to an end, the European Union's regulation on data protection, known as GDPR, will be retained in domestic law through the European Union (Withdrawal) Act 2018. Last year the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 were made. They made minor changes to the retained GDPR under the Data Protection Act 2018, to ensure that UK data protection law would continue to operate on exit day.

The statutory instrument before the Committee today makes limited amendments to those regulations. The majority of the changes are updates of exit day references to read "IP completion day". The SI will also revoke some EU legislation that would have no practical effect if it were to be retained under the European Union (Withdrawal) Act 2018 at the end of the transition period.

There are a small number of other changes, which relate to the transitional provisions for international transfers of personal data. At the end of the transitional period UK organisations will be able to transfer personal data outside the UK if it is covered by an adequacy regulation, an appropriate safeguard, or an exception. Currently UK organisations can freely transfer personal data to EU and European economic area member states and to non-EEA countries for which the EU Commission has made adequacy decisions.

The regulations that I have referred to continue that position on a transitional basis. For clarity, the relevant adequacy decisions are listed. The measure before the Committee updates that list to reflect recent developments, adding the EU's adequacy decision for Japan, and removing the reference to the adequacy decision for the US privacy shield. These amendments are not substantive, and are entirely in keeping with the original intention of the main regulations—namely, to ensure the continued free flow of personal data between the UK and third countries that have already been found to meet the requisite standards for data protection.

Binding corporate rules are an internal code of conduct operating within a multinational group, which has been approved by EU data protection regulators, to enable personal data to be transferred within the global group. The main regulations preserve pre-GDPR binding corporate rules that were previously authorised by the Information Commissioner as a valid transfer mechanism after the transition period. However, a subset of pre-GDPR binding corporate rules currently relied on by organisations with data flows in the UK may have received authorisation only from EU supervisory authorities. The SI before the Committee makes provisions that will allow UK-based group members to use such rules as a valid transfer mechanism if they obtain approval from the Information Commissioner within six months of the end of the transition period.

The main regulations also provided a legal basis for the continued free flow of personal data from the UK to the EU, falling within the scope of the law enforcement directive, otherwise known as the LED. The approach adopted in the main regulations was to transitionally deem EU member states and Gibraltar as adequate.

Since the main regulations were made, the Home Office has established that Norway, Iceland, Liechtenstein and Switzerland have also transposed the law enforcement directive into their domestic law, which enables data sharing between authorities in the UK and law enforcement agencies within these countries. In order that law enforcement co-operation and data sharing can continue as it does now, following the end of the transition period, this instrument adds these EEA states and Switzerland to the list of countries that will be treated as adequate on a transitional basis.

Finally, I turn to the revocation of the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019. In 2019, an additional SI was made to amend the main regulations to reflect the arrangements made for personal data transferred from the UK to privacy shield companies in the US. As the CJEU has invalidated the adequacy decision, the amending regulation no longer has any practical effect and, therefore, this regulation revokes that amending regulation before it comes into force.

As I have set out, these regulations address deficiencies in our data protection regime resulting from the UK's leaving the EU at the end of the transition period. I commend the regulations to the Committee.

2.36 pm

Chi Onwurah (Newcastle upon Tyne Central) (Lab): It is a pleasure, Mr McCabe, to serve under your chairship for this important statutory instrument. I thank the Minister for his opening remarks. I also state

for the record that although I was as dismayed as most people by all the emails that invaded our inboxes from organisations explaining their data privacy policies when the general data protection regulation took effect in 2018, I was pleased that data protection was finally beginning to be taken seriously and coming to the attention of the vast majority of people—even in that most irritating way.

Data is the business model of the internet age. It is often referred to as “the new oil”. I do not like that because we have seen what oil extraction has done, both to the environment in countries such as Nigeria and to the planet with carbon emissions. We want to make sure that the impact of data is more constructive in the short and long term. It is certain that there is an impact. As more and more aspects of our lives move online—and the pandemic has accelerated that migration—we all excrete a trail of data and create a data doppelgänger, which can be used to empower and inform us or to control, sell to and disempower us. Data privacy, data rights and data flows are therefore of critical importance to all of us.

Depending on any deal, which may or may not be signed—we still do not know—by the Government when the UK leaves the transition period, our data and data protection will no longer be subject to the European Union’s GDPR law. Instead, we will have transposed EU GDPR into UK GDPR. The direction in which the UK takes GDPR will have a wide-ranging impact. Cross-border data flows are now an absolute requisite of trade, with businesses reliant on their ability to transfer personal data about their customers or workforce to offer goods or services and run even basic internal processes such as cloud-based email or file storage. Those all involve data flows, but that is especially true of digitally intensive sectors—telecommunications and financial services, which account for 16% of UK economic output and a quarter of total exports, according to techUK.

As the Minister set out, the SI amends and revokes areas of legislation to ensure that the European Union’s GDPR law is translated into UK GDPR law in time for the end of the transition period, as agreed under the withdrawal agreement. The EU GDPR will become UK legislation on IP completion day and, as such, will become the UK’s GDPR. It is then immediately corrected by today’s SI.

As the Minister set out, the SI seeks to ensure that the legal framework for data protection within the UK continues to function correctly after the transition period. The changes in the SI update the date on which the DPPEC come into force from the start—exit day—to the end of the transition period, IP completion day, in effect applying EU case law during the past nine months, ensuring that personal data can continue to be transferred to third countries as it could immediately before exit day. And they set out revised transfer provisions for law enforcement data to include the addition of EEA countries.

The current transitional mechanism does not apply for any EU adequacy decisions that are repealed or suspended immediately before IP completion day, as amended by this instrument. On 16 July 2020, in case C-311/18, commonly referred to as Schrems II, the Court of Justice of the European Union declared one such decision, the Privacy Shield agreement with the USA, to be invalid. Therefore, the transitional mechanism will not apply for that decision, and this SI removes Privacy Shield from the list of transitional adequacy provisions that the UK will roll over.

The SI incorporates European Union decisions on the adequacy of third party countries in UK domestic law. Data adequacy is a status granted by the European Commission to countries outside the European economic area that provide a level of personal data protection comparable to that provided by European law. When a country has been awarded the status, information can pass freely between it and the EEA without further safeguards being required.

However, despite the UK’s application of the GDPR and implementation of the law enforcement directive under the Data Protection Act 2018, there is no guarantee that we will be awarded an adequacy decision. The European Court of Justice, which can strike down any adequacy decision approved by the Commission, has already twice ruled that the UK’s handling of personal data is not in line with European Union law, so can the Minister tell me what discussions he has had with the European Union about the likelihood of the UK receiving data adequacy recognition? I am sure that he recognises that many businesses are very concerned to have some reassurance and some certainty in this regard.

Even if the UK does manage to secure an adequacy agreement before the end of the transition period, there is no guarantee that we will keep it. It will be vulnerable to being overturned by the European Court of Justice, so can the Minister promise us that the UK’s handling of personal data will remain in line with our legal obligations that arise from any agreement with the European Union, and can he set out what impact he envisages—I know that he is well versed in these areas—European Court of Justice rulings might then have on UK GDPR law? Will they, as it were, remain supreme following the end of the transition period?

Those are the things that the SI does, but there are some things that it does not do. The Government have not been clear or forthcoming about their data management strategy. The shift of public sector data management from the Department for Digital, Culture, Media and Sport to No. 10 in July—as I understand it, at the behest of Dominic Cummings, no longer of this parish—raised many questions as to the direction of the Government’s handling and use of public data.

The national data strategy, which is undergoing a consultation that closes next week, talks a lot about the role that data can play in driving economic growth, but there is nothing about data rights, duties and obligations on the huge tech platforms that use and misuse so much of our data, or discussion of a regulatory framework for data. Content created by the tech platforms uses people’s data to promote disinformation, fake news, extremism, hatred and other harmful material, while data-driven business models place ever more extreme content in front of our eyeballs.

I recognise that the statutory instrument is limited, but it would be helpful if the Minister said something about the extent to which he sees our GDPR evolving, addressing in particular the issue of data rights. That would help us to understand its impact. The SI does nothing to address long-term alignment and divergence decisions. The explanatory memorandum mentions “UK GDPR”. Does that language indicate that the Government intend to diverge from European Union GDPR?

As the UK begins to sign trade deals across the world, UK GDPR may be altered. The recent Japan trade deal made reference to facilitating data transfers and could allow them to go via third countries such as

[*Chi Onwurah*]

the US, which might have different data regulations. Will the Minister commit to ensuring that data protections and treatment are not traded away and that our data protection regulations remain in line with European Union minimum standards, to ensure validity for third-nation adequacy benefits?

That is already an issue, as the privacy shield adequacy agreement with the US has been invalidated, and the European Union adequacy agreement with Japan, as I understand it, has no practical effect in the UK. How, then, will adequacy be reflected in our ability to negotiate future trade agreements? Are further decisions of this type likely and how will they be reflected in UK law?

Finally, the Labour party is passionate about ensuring that our citizens have control of their own data. We have proposed a digital charter to put people's real selves back in control of their digital selves. I would appreciate it if the Minister told us how he plans to ensure that agreements with other nations do not provide a back-door way to undermine GDPR. We will not oppose the instrument as it is necessary, but we have concerns about the specifics, and we think assurances must be given to businesses and others about our data privacy and control.

2.48 pm

Mr Whittingdale: I am grateful to the hon. Lady for indicating that the Opposition do not intend to oppose the regulations and for her remarks. I am tempted to say that we should stop meeting like this, but I think we may be doing so again in further Committees.

The hon. Lady and I absolutely agree about the importance of data in fuelling economic growth and innovation. She does not like the expression "new oil" in that context, and I understand why, but I am not sure that her suggestion about people going around excreting a trail of data was much more preferable an analogy. Nevertheless, data is of increasing importance, and the Government are keen to ensure that we reap the maximum benefit from it to create an economy driven by innovation and growth, based on the free flow of data. At the same time, we absolutely recognise the importance of data protection, which is, as she said, underpinned by GDPR, a set of EU regulations.

The hon. Lady referred to the fact that we are still in negotiation with the EU Commission about adequacy. In our view, there is no reason that we should not be granted adequacy—after all, our data protection regime is one that the EU formulated—but that is a matter ultimately for the Commission to decide. Certainly, the time left before the end of the transition period is reducing and this is therefore challenging, but we are still optimistic that it can be achieved. We have indicated to business that it is sensible to put in place the mechanisms necessary to ensure that data can continue to flow from the EU to the UK should adequacy not be achieved.

I am sure the Committee would have been disappointed if the hon. Lady had not mentioned Schrems II, which we all think about a great deal. Schrems II resulted in some quite tricky decisions, not just for the UK, because we are bound by the Schrems II judgment that negated the privacy shield, but it creates equal challenges for the EU, which is something the EU is working on; the Information Commissioner's Office is still in conversation;

and we hope to find a mechanism to allow the flow of data between EU member states, the UK and the USA to continue.

The hon. Lady is right that, even if we achieve adequacy, this is an ongoing process. We would not be negotiating as hard as we are to achieve adequacy if we intended to do anything shortly afterwards that resulted in our losing it again. On the other hand, we wish to take advantage of the fact that we will be responsible for our own data protection regime, and we wish to explore ways to facilitate the flow of data between companies and to drive growth forward. That is an opportunity, since we will no longer be bound by the Court of Justice of the European Union rulings, although in terms of adequacy decisions we will need to watch developments in the EU. Should those rulings change things, there might be implications for its attitude to our adequacy.

We certainly have no intention of doing anything that results in a loss of adequacy. The national data strategy mentioned by the hon. Lady is intended to consult very widely all those who potentially have an interest in the matter—companies that use data, privacy campaigners, stakeholders and so on—to find ways in which we might improve the UK's data regime. She referred to the Opposition's suggestion of a digital charter. I hope she has responded to the national data strategy, as we are obviously interested in any ideas that she has.

On trade agreements, which the hon. Lady also talked about, it is true that, for instance, the UK-Japan trade agreement contains data provisions that go beyond the EU-Japan agreement, and we regard that as a considerable achievement. However, nothing in the agreement undermines the data protection regime in this country. Indeed, the agreement makes it absolutely clear that both sides are able to maintain a legal framework that provides for the protection of personal information. The trade agreement with Japan will, we hope, result in a freer flow of data between the UK and Japan, but at the same time not undermine GDPR and our existing protection.

Chi Onwurah: I thank the Minister for his responses and his genuinely seeking to answer my questions, which is something of an experience for me. We have an agreement with Japan, which means data will be allowed to go to Japan. Japan has an agreement with the US, so data is allowed to go to the US. That undermines our conditions on data flowing from the UK to the US if they do not meet the European Union adequacy rules. That is what I meant by a back door.

Mr Whittingdale: I understand the hon. Lady's concern, but I do not think it is justified. There is nothing forcing any company to transfer data from the UK to Japan or any other third country. We seek to remove unnecessary obstacles that impede that flow, but that does not undermine the requirements on UK-based companies to comply with the existing data protection regime. Indeed, that is spelt out clearly in the agreement. We do not believe that that is a risk, but it is something we continue to attach priority to, and we will keep it in mind for the future trade agreements that we are hopeful of striking.

I hope I am answering the points that the hon. Lady made. The point she made at the end of her remarks was about the obligations on the tech platforms, and she talked about disinformation and fake news. As she

will be aware, the Secretary of State had a recent roundtable specifically to talk about the efforts made by the tech platforms to address the problem of disinformation about a potential covid vaccine. She will also know that the issue of obligations on tech platforms will be addressed through the online harms legislation that we still expect in the near future.

I hope I have answered the hon. Lady's questions and I commend the regulations to the Committee.

Question put and agreed to.

2.56 pm

Committee rose.

