Eleonor Duhs – Written Evidence (DAT0005)

Written evidence on inquiry into UK-EU data adequacy

This evidence is intended to provide further information and citations for my oral evidence given on 26th March 2024.

What is your assessment of the existing adequacy arrangement underpinning data flows between the UK and the European Union?

The International Chamber of Commerce has said that the benefits of trade depend on the trusted flow of data between countries. Data transfers are estimated to be on course to contribute 11 trillion dollars to global GDP by 2025, which exceeds the global trade in goods. The free flow of data from the EU to the UK is also crucial for trade and in the UK many sectors of our economy depend on this free flow of data. Examples include finance, banking, retail and hospitality. The free flow of data is important to both large multinationals as well as SMEs who provide goods or services across borders.

At its core EU and UK data protection law is a detailed working out of Article 8 of the European Convention on Human Rights – the right to a private and family life. The human rights core of our data protection legislation is crucial. Human rights law is the correct starting point when it comes to thinking about data protection standards, particularly in the age of AI. But the way in which the GDPR translates that right into a set of overly complex and unrealistic rules is regrettable and needs to be overhauled. But adequacy constrains the UK from doing that in a meaningful way. Data protection reform needs to happen with international partners at an international level.

What is your assessment of the value of the EU's adequacy decisions to UK organisations?

The EU's adequacy decision is crucial for avoiding significant red tape for UK businesses. The New Economics Foundation and UCL European Institute wrote a report published in November 2020 which looked at what would happen if the UK did not receive data adequacy from the EU on departure from the bloc.

They estimated the cost at between £1bn and £1.6bn for UK businesses. This extra cost stemmed from additional compliance obligations such as putting standard contractual clauses in place between the data exporter in the EU and the data importer in the UK. This was a conservative estimate. In terms of how that broke down the costs would be as follows:

- £3,000 for a micro business

- £10,000 for a small business
- £19,555 for a medium sized business
- £162,790 for a large business

This overall figure of between £1 billion and £1.6 billion represents money that companies would otherwise be free to spend to meet the requirements of the business by, for instance, investing in new equipment, staff, or processes, but instead would have to be channelled into compliance activities or additional costs for goods and services, due to EU-UK data flows disruption.

One of the most significant changes since the Schrems II case is the requirement that organisations conduct transfer risk assessments in order to ensure that the standard of protection for the data will be "essentially equivalent" to the protections which apply in the EU. This involves a "mini-adequacy assessment". Organisations have to apply the same test as the European Commission when it conducts an adequacy assessment. The test is set out at Article 45(2) of the GDPR and includes consideration of the following matters in relation to the jurisdiction to which the data is to be transferred:

- the rule of law
- respect for human rights and fundamental freedoms;
- relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation,
- the existence and effective functioning of one or more independent supervisory authorities in the third country; and
- the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

☐

How are the General Data Protection Regulation and the Law Enforcement Directive working in practice? What extra costs do they impose on businesses?

Dr Winfried Veil has done some analysis of the burdens which the GDPR regime imposes. These include:

- 82 balancing tests, including 30 necessity tests
- 77 references to the data subject's rights and freedoms .

To have a regime which applies to every business in Europe and which nobody can be confident they comply with creates a serious problem with the rule of law. In a democracy we should be able to expect that law will be drafted in a way which is clear and that we can adjust our behaviour to comply with it. If the law is so complex and onerous that everyone is in breach that is anti-democratic.

There is evidence that the GDPR has imposed costs. There has been some very recently-published research on this from Frey and Presidente entitled 'Privacy regulation and firm performance: estimating the GDPR effect globally'. The researchers state that digital technology companies have been most impacted by GDPR. Technology companies targeting EU markets experienced a 2.1% reduction in profits. GDPR also increased non-operating expenses as well as firms' wage bills. They also site previous research which suggests that SMEs have faced "significant challenges due to GDPR across various dimensions" and that "smaller companies have suffered more in terms of profitability."

The costs outlined above have to be balanced against the impact of a lack of investment in data protection compliance. Experts including the former information commissioner Elizabeth Denham in her response to the government's consultation on data protection reform said that if individuals did not trust how their data was being used then they would not hand it over. Dr Jeni Tennison made a similar point when giving evidence in the House of Commons on the data protection and digital information bill. She said "I am concerned about the gradual drift of reducing trust in the public sphere when it comes to the use of data by Governments and organisations. In some ways, I am more concerned about this leading to people not adopting technology and opting out of data collection because they are worried about what might happen. That would hold us back from the progress and the good uses of data that I would really like to see." (HC Deb 10 May 2023, vol 733, col 36).

How would you assess the overall performance and effectiveness of the Information Commissioner's Office (ICO) as the UK's independent data regulator?

Research by Professor David Erdos at the University of Cambridge highlights what some consider to be evidence of a poor track record of enforcement. In 2021-22 The ICO did not serve a single GDPR enforcement notice, secured no criminal convictions and issued only four GDPR fines totalling just £183,000 despite the fact that it received over 40,000 data subject complaints.

What factors could influence the next European Commission when deciding whether to renew its data adequacy decisions for the UK in June 2025?

The European Commission will do everything it can to continue data adequacy for the UK. EU businesses will want to continue to be able to send data to the UK without having to worry about standard contractual clauses, risk assessments and putting in place supplementary measures to protect the data. Further, if the UK's data adequacy doesn't continue then the bar for adequacy will be set impossibly high.

It's worth noting that adequacy isn't solely a legal test for the European Commission – it has a strong political dimension. For example, the Commission's communication of 10th January 2017 sets out criteria which the Commission will consider when deciding which third countries it should assess for adequacy. The criteria are:

- the extent of the EU's commercial relations with the third country (including the existence of ongoing negotiations around a free trade agreement),
- the extent of personal data flows from the EU to the third country, reflecting geographical and/or cultural ties,
- the role the third country plays in the field of privacy and data protection, and
- the overall political relationship with the third country in question.

These political considerations play a very important role in either conferring adequacy but also continuing existing adequacy decisions, as evidenced by the approach taken by the European Commission in its report on existing adequacy decisions.

☐

What factors could the Court of Justice of the EU (CJEU) consider if the legality of the EU-UK adequacy decisions were challenged?

The CJEU would look at whether the standard of protection of personal data in the UK is essentially equivalent to that in the EU.

The UK is at a disadvantage here: if its data protection law was completely different from the EU's then it would be much more difficult to weigh up whether it was essentially equivalent or not.

Where the UK is clearly dropping its standards then it's quite easy to establish that the UK doesn't have an essentially equivalent standard of protection.

There are four areas of risk to highlight. If the DPDI Bill goes through as drafted then there are likely to be more:

1. standard of protection for data subjects (even without the changes made by DPDI Bill)

2. Deletion of the concept of EU fundamental rights, and with it the potential loss of CJEU case law which interprets data protection law

3. Independence of the ICO

4. The UK's obligations under international law, including

a. UK's adherence to the ECHR

b. Ratification of Council of Europe Convention 108+

1. Standard of protection for data subjects (without the changes made by DPDI Bill)

The EU's current adequacy decision for the UK does not apply to the area of immigration. This is because at the time of the adequacy decision a challenge was being brought to the immigration exemption in paragraph 4(1) of Schedule 2 to the Data Protection Act 2018. The challenge was based on the argument that the immigration exemption was too broad and was therefore contrary to the requirements of Article 23(2) of the UK GDPR. The Court of Appeal ruled that the immigration exemption was unlawful and disapplied it on the basis of the retained principle of the supremacy of EU law. The principle of the supremacy of EU law was deleted at the end of 2023 through the operation of the Retained EU Law (Revocation and Reform) Act 2023 and this kind of challenge is no longer possible.

It is clear that none of the exemptions under Schedule 2-4 of the Data Protection Act 2018 were drafted in such a way as to comply with the requirements of Article 23(2) of the UK GDPR. This issue is likely to become relevant when the European Commission reassesses the UK's data adequacy next year. The significant discrepancies in the level of safeguards under the immigration exemption as compared with those provided under any of the other exemptions set out in Schedule 2-4 of the Data Protection Act 2018 could also be cited in any challenge to UK

data adequacy before the CJEU. The argument would be that only in the area of immigration are the protections for data subjects "essentially equivalent" to those under the EU regime and therefore that the UK's data adequacy decision is invalid.

2. Deletion of the concept of EU fundamental rights

The Retained EU Law (Revocation and Reform) Act 2023 deleted the concept of EU fundamental rights from the UK statute book. That created a problem for data protection law because the GDPR explicitly states in the first line of the first recital that the protection of personal data is a fundamental right. Fundamental Rights are therefore the underpinning foundation of the law. The government therefore brought forward secondary legislation at the end of last year to ensure that references to fundamental rights and freedoms in the UK GDPR did not become meaningless. The secondary legislation said that references to fundamental rights and freedoms in the UK GDPR should be read so as to refer to the right to a private and family life as protected through Article 8 of the ECHR. But it's not clear that the right under Article 8 of the ECHR is the same as the fundamental right to the protection of personal data in the EU legal order. In the case of Watson from 2015 the High Court stated that the EU right to the protection of personal data was more specific and went further than Article 8 of the ECHR . That may mean that the deletion of EU fundamental rights has resulted in a lower standard of protection of personal data in the UK than in the EU. There is also uncertainty relating to assimilated case law because in numerous cases the CJEU has used the fundamental right to the protection of personal data to interpret the EU data protection regime. If that right is gone then it is far from clear that the case law still applies. That creates legal uncertainty: The potential loss of assimilated case law could also create a lower standard of protection of personal data in the UK as compared with the EU.

3. Independence of the Regulator

The independence of the Regulator is key in data protection law – it is mentioned in Article 8(3) of the EU Charter of fundamental rights which states: Compliance [with rules on data protection] shall be subject to control by an independent authority. One of the things the DPDI Bill removes is references to an independent regulator for data protection where the SoSo is considering whether a third country should have UK adequacy. This is an area of significant vulnerability for the UK, should there be a challenge to the adequacy of the UK regime.

4. International commitments

- Recital 19 to the UK's current adequacy decision highlights that the UK's adherence to ECHR and Council of Europe convention 108 are "a particularly important element"of the UK's legal framework assessed in the decision. The problems here are:

o If the next election is fought and won on a manifesto to leave the ECHR then I think that would have consequences for data adequacy and for the free flow of data from the EU to the UK and would be raised in any challenge to UK data adequacy; and

o Council of Europe convention 108 has been modernised to reflect the GDPR. The UK has not ratified the modernised convention which Professor David Erdos considers is likely to enter into force in the next 2 years. If the UK does not ratify the modernised convention then this supports arguments about the UK not reaching the standard of essential equivalence with the EU regime.

- All of these factors potentially lead to a loss of a finding of essential equivalence and therefore the loss of the UKs data adequacy in a challenge before the CJEU..

☐

How would you assess the possible impact of proposed UK rules on automated decision-making and the use of Artificial Intelligence on data adequacy?

This is an area where the UK is lowering standards of protection. Using solely automated decision making for taking important decisions about individuals is prohibited under the GDPR. This is subject to limited exemptions, for example where individuals have given explicit consent or where automated decisions are necessary for the entering into or the performance of a contract between the data subject and the data controller. Where automated decision-making is permissible, safeguards need to be in place, such as the right to obtain human review and contest the decision.

Under the Data Protection and Digital Information Bill this prohibition is removed except for where the data being processed is special category data (for example data about an individual's health or ethnicity). However, the right to obtain human review and contest the decision will remain.

Removing the current restriction and allowing automated decision-making takes the UK in the wrong direction. Further, Ministers are giving themselves very broad powers in the Bill to completely rewrite the protections from automated decision-making that will remain, potentially removing them altogether for certain types of automated decisions. This

is not appropriate. The Delegated Powers and Regulatory Reform Committee says that Ministers should not be able to lower protections using secondary legislation. This links to a broader point about how we legislate in the digital age. Giving more and more powers to Ministers is completely the wrong way to deal with the speed of technological innovation. It is not democratic.

Watering down safeguards in the context of automated decision-making removes crucial protections in the age of AI and is clear evidence that the UK's standards of protection of personal data are dropping. These changes could be cited in any challenge to UK data adequacy by the CJEU and clearly evidence that in this context UK data protection rights are lower than rights in the EU.

Examples from the Communication Worker's Union of the effects of AI on the workforce (even with relatively strong protections under the UK GDPR as currently drafted) illustrate the significant dangers posed by the use of this technology in terms of indivdiuals' rights and dignity at work:

In a hi-tech logistics company a newly appointed manager, straight from university, without human training made an expense claim incorrectly, rather than have human oversight, a computer authorised the expenses, the first the employee knew there was an error was when he was called in for a dismissal hearing. The company thought there was nothing wrong with relying solely on computer based training and computer oversight, their attitude was that this error showed the problem was with their human employees.

The introduction of tracking technology in a communication company caused a great deal of trouble for us, it was brought in alongside a new productivity system and aggregated data from many sources. Although the agreement on introduction stated it would not be used for disciplinary purposes, the implementation was very different.

Some early examples were almost humorous, such as workers being brought in to explain why they stopped at traffic lights. But soon as the computer generated reports highlighted time spent in the depo and simple matters of dignity were under attack such as workers being pressured not to use toilets in work time, not to make use of welfare facilities in order to game the report so that a managers red box turned to a green box on his report. Later systems would direct technicians to specific work points by the machine, often it was incorrect and no match for years of experience and local knowledge, the company knew this and allowed deviation whilst it worked - but if for any reason your productivity was low your failure to follow the machines commands was

noted and then monitored as you started a plan to improve or be exited from the business.

One system recently under consideration by a broadband provider was an inwards facing vehicle camera, with the ability to allow managers to view a video stream, listen to conversations and use AI to text managers if it detected you holding a mobile phone, or report you for yawning. Offers by the union to accept forward facing and vehicle reversing cameras were declined without us accepting AI employee surveillance camera – despite assurances that the scheme was going to be introduced for employee and public safety. The company were not able to provide any examples or statistics to show the safety issue they were addressing or how the technology could help. This scheme was quickly abandoned when the union notified staff and announced a campaign against the intrusive technology.

AI tools can also provide a real-time assessment of your conversations, call centre workers working under these conditions in Wales reported being measured on speaking too slowly, speaking too fast, told to pause more or don't pause so long amongst a myriad of other metrics this AI measured and ranked them emotionally quantifying their empathy and positivity. Some members have reported losing around £500 per month for not using key words or not trying to up sell products on calls where a human knows the customer is not interested in sales.

☐

What implications, if any, would a no or disrupted UK-EU data adequacy scenario have?

Baroness Hayter asked the following question (Q15):

I left a question dripping on the civil side. Do you have any experience of that that you wanted to feed to the Committee afterwards? When we were doing this some time ago, it was not just criminal law. In family law, there is access to children, maintenance, attachment of earnings and an enormous number of privacy issues. It would be interesting to know how any change to adequacy would affect that. I hear we have gone back into Hague now. I am not on top of it any more. If you would like to submit something, we would probably welcome that.

I am grateful to Gareth Oldale, Partner, Technology, IP and Data for TLT LLP for the following answer:

Instinctively it doesn't feel to me that a loss of adequacy status from the EU – whilst catastrophic in lots of other ways – would be quite so

damaging when it comes to dealing with domestic intra-UK family law matters such as access to children, maintenance, attachment of earnings etc. I say this as principally one would expect the extent of any data transfers to be largely within the UK or between UK entities (e.g. between two UK law firms). Two immediate caveats to that which occur to me however, where the loss of adequacy status could have more of a profound effect in a family law context, are:

1. Dealing with divorce proceedings (or access to children etc) in matters where one parent lives in the UK and another in an EU member state. I am sure this happens on a fairly frequent basis, e.g. on the island of Ireland where one parent may live north and the other south of the border. Equally if one parent has emigrated to Spain, then transferring personal data from law firm A in the UK to law firm B in Spain would clearly be more challenging in the absence of an adequacy decision.

2. Providers of family law services (including law firms, mediators, domestic violence charities etc) which rely on suppliers based in the EU for the delivery of services which are utilised to process personal data of customers/service users. For example, if law firm A in the UK has an outsourced IT helpdesk in Poland which has access to client records, then again the absence of an adequacy decision would put an additional burden on law firm A to enable those international transfers to Poland to continue.

Eleonor Duhs

Bates Wells

1st May 2024

Received 2 May 2024