Douwe Korff & Ian Brown

The inadequacy of UK data protection law
Part One: General inadequacy

with comments on the adequacy decisions on Guernsey, Jersey and the Isle of Man & implications for other countries and territories, including Gibraltar & EU Member States

The first part of a two-part submission to the European Union bodies assessing whether under the EU General Data Protection Regulation the United Kingdom should be held to provide "adequate" protection to personal data.

Cambridge/London, UK

9 October 2020

About the authors:

Douwe Korff is Emeritus Professor of International Law at London Metropolitan University and an Associate of the Oxford Martin School of the University of Oxford, a Visiting Fellow at Yale University (Information Society Project), and a Fellow at the Centre for Internet and Human Rights of the European University of Viadrina, Berlin. Among many other publications, he wrote the Council of Europe Commissioner for Human Rights' *Issue Paper* on The Rule of Law on the Internet and in the wider digital environment (2014), available at: https://rm.coe.int/ref/CommDH/IssuePaper(2014)1. He was also the lead author (with Ben Wagner, Julia Powles, Renata Avila and Ulf Buermeyer) of Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes, a comparative report covering Colombia, DR Congo, Egypt, France, Germany, India, Kenya, Myanmar, Pakistan, Russia, South Africa, Turkey, UK and USA, prepared for the World Wide Web Foundation (2017), available at: https://ssrn.com/abstract=2894490

Website: http://douwe.korff.co.uk

Ian Brown is visiting CyberBRICS professor at Fundação Getulio Vargas (FGV) Law School in Rio de Janeiro, and an ACM Distinguished Scientist. He was previously Principal Scientific Officer at the UK government's Department for Digital, Culture, Media and Sport; Professor of Information Security and Privacy at the University of Oxford's Internet Institute; and a Knowledge Exchange Fellow with the Commonwealth Secretariat and UK National Crime Agency. His books include Cybersecurity for Elections (2020, Commonwealth Secretariat, with Marsden/Lee/Veale), Regulating Code (2013, MIT Press, with Marsden), and Research Handbook on Governance of the Internet (ed., 2013, Edward Elgar). He co-founded and served on the boards of European Digital Rights, Open Rights Group, the Foundation for Information Policy Research and Privacy International; and has written for *The Financial Times* and *The Guardian*. He is a fellow of the British Computing Society, Open Forum Europe, and the International University of Japan.

Website: https://www.ianbrown.tech/about/

Douwe Korff & Ian Brown were the joint authors of Terrorism and the Proportionality of Internet Surveillance, European Journal of Criminology, March 2009, available at: SSRN: http://ssrn.com/abstract=1261194

Both have testified as experts on surveillance or surveillance law to various bodies including (between them) the Parliamentary Assembly of the Council of Europe (PACE), the European Parliament (LIBE Committee) and national parliaments including the German *Bundestag* and the UK House of Lords. Brown acted as an expert witness for the UK Investigatory Powers Tribunal and European Court of Human Rights in cases relating to UK surveillance practices.

Acknowledgments:

The authors are grateful to **Chris Pounder, Judith Rauhofer**, and **Pat Walshe** for reviewing their summaries of the UK legal regimes relating to data protection.

We are also happy to acknowledge our reliance in several respects on the excellent analyses by **Chris Pounder** and **Graham Smith** at:
http://www.amberhawk.com/ (Chris Pounder)
http://www.cyberleagle.com/ (Graham Smith)

Any errors of course remain solely ours.

CONTENTS

- o – O – o -

1. Introduction

Under the EU General Data Protection Regulation (GDPR), flows of personal data subject to that instrument[1] are allowed without restraint between Member States of the European Union and the European Economic Area (EEA),[2] and between EU/EEA Member States and non-EU/EEA countries (so-called "third countries") that provide an "adequate" level of protection to such data (Articles 1(3), 44 and 45 GDPR).

In its *Schrems I* judgment, the Court of Justice of the EU (CJEU) has held in the latter respect this means the third country in question must ensure "essentially equivalent" protection to the data.[3] If a third country does not provide "adequate"/"essentially equivalent" protection, personal data may only be transferred from the EU/EEA to that country if "appropriate safeguards" are put in place by the exporter in the EU (with the help of the importer in the third country), such as so-called Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs, used for data flows within an international corporation or group of corporations).

Now the United Kingdom is no longer an EU Member State, and after the post-Brexit transition period ending on 31 December 2020, personal data will therefore not be allowed to flow freely from the EU to the UK unless the European Commission adopts a decision under Article 45 GDPR that the UK ensures an adequate level of protection.

In section 2 of this first part of our analysis, we outline the requirements for a positive adequacy decision, with reference to the *Schrems I* judgment and the Article 29 Working Party's "Adequacy Referential" on the issue (and brief references to our later findings *re* the UK), and the process for adopting such a decision. In section 3, we note a range of issues that raise serious doubts about whether UK data protection law after the post-Brexit transition period can be deemed "adequate".

In Part Two, we assess the compatibility of the UK legal regimes for surveillance and bulk data collection with EU law, including the Charter of Fundamental Rights and the "general principles of Community law", which derive from the European Convention on Human Rights and "the constitutional traditions common to the Member States" (Article 6(3) TEU), and therefore with the GDPR. The EU is itself required to become a party to that Convention (Article 6(2) TEU) (although that process is somewhat stalled), while the UK is, for the time being, a State Party, albeit sometimes a rather reluctant one.

---

[1] Personal data that are processed in relation to the activities of the law enforcement agencies of the EU Member States are subject to a separate instrument, the Law Enforcement Directive, which contains similar transfer rules. See: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4 May 2016, p. 89–131, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG
However, this submission is limited to the question of whether, in relation of transfers of personal data that are subject to the GDPR from the EU/EEA to the UK after the post-Brexit transition period, the UK can be deemed to provide "adequate" protection (as discussed in the text).

[2] The EEA consists of the EU Member States plus Iceland, Norway and Liechtenstein. EU data protection law including the GDPR applies to all EEA Member States. In this submission we will, after the initial paragraph, for simplicity sake refer to the EU, but this should be read as referring to both the EU and the EEA.

[3] CJEU, Grand Chamber judgment of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* ("*Schrems I*"), para. 73, available at: http://curia.europa.eu/juris/liste.jsf?num=C-362/14

In that second part, we set out the legal regimes for mass surveillance and bulk data collection as elucidated by the European Court of Human Rights (ECtHR) in its *Big Brother Watch v. the UK* judgment, with that court's assessments of those regimes (while also noting the ECtHR did not examine some wider arrangements); and note the changes made to two of the regimes since the *BBW* judgment. We summarise the standards set by the Court of Justice of the European Union (CJEU) in relation to mass surveillance and bulk data collection in its *Tele2/Watson*, *Digital Rights, Schrems II, La Quadrature du Net* and *Privacy International* judgments; discuss the "European Essential Guarantees" adduced by the Article 29 Working Party in that regard; and assess the UK surveillance regimes (including the arrangements not assessed by the ECtHR) in the light of those standards. We conclude they do not meet the CJEU/WP29 standards. We also provide some brief comments on the implications of our findings for the adequacy decisions on Guernsey, Jersey and the Isle of Man and for the situation in relation to Gibraltar, and on the implications for other countries, including EU Member States.

2. EU Adequacy decisions and requirements for onward transfers

2.1 Requirements for a positive adequacy decision

2.1.1 General requirements

Article 44 GDPR sets out the "general principle for transfers" of personal data to non-EU countries (so-called "third countries"), as follows:

Article 44

General principle for transfers

> Any transfer of personal data which are undergoing processing[4] or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45(1) stipulates that

> A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

The CJEU has held "adequate protection" must be read as requiring "essentially equivalent" protection to that accorded by EU law.[5]

Article 45(2) sets out the main matters that the Commission must take into account in its assessment of the adequacy of the law in a third country:

> When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
>
> (a) 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, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

[4] Note that "processing" here (and elsewhere in the GDPR) has a very broad scope, it covers: "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*" (Article 4(2) GDPR)

[5] See footnote 3, above.

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) 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.

Following the *Schrems I* "essential equivalence" test, the WP29 expanded on the requirements for an adequacy decision in its "Adequacy Referential", the final version of which was adopted in November 2017 and endorsed by the European Data Protection Board at its first meeting in May 2018.[6] Briefly, in line with the stipulations in Article 45(2), adequacy assessments must comprise the following three elements:

- an assessment of whether the law relating to privacy/the processing of personal data in the third country provides "essentially equivalent" protection to such data as is provided in the EU, in that they reflect the substantive "core content" elements of EU data protection law as summarised in Article 8(1) and (2) of the Charter of Fundamental Rights and further elaborated in the GDPR;
- an assessment of whether the law in the third country provides for "procedural/enforcement" guarantees that are "essentially equivalent" to those provided for Article 8(3) of the Charter and also further elaborated in the GDPR;

and, more broadly:

- an assessment of whether the rule of law and respect for human rights and fundamental freedoms is ensured in the third country concerned.

[6] Article 29 Working Party, Adequacy Referential, adopted on 28 November 2017, as last revised and adopted on 6 February 2018 (WP254rev01), available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
EDPB endorsement:
https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf
The Adequacy Referential replaced a very early WP29 Working Document – Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive (WP12), adopted on 24 July 1998, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf

In section 3, below, we will show that there are serious doubts as to whether the UK meets the first two of the three general requirements set out above. In relation to the third set of requirements, we will, in Part Two, address the question of access to personal data by the UK's national security agencies that arises in that context. That important matter aside, it will suffice to note here in relation to that third set of requirements that the UK has put its adherence to the rule of law in doubt by introducing legislation - the Internal Market Bill – that, as the Northern Ireland Secretary, Brandon Lewis, explicitly acknowledged in Parliament, breaks international law "in a very specific and limited way";[7] and that, again, the UK Government has raised doubts about its continuing adherence to the ECHR.[8]

2.1.2 Requirements concerning access to EU personal data by agencies of the data importing country

As Article 45(2)(a) GDPR, quoted above, makes explicitly clear, the last of the above issues includes the question of whether the laws and rules in the third country relating to "*public security, defence, national security and criminal law and the access of public authorities to personal data*" are in line with the rule of law, and respect human rights and fundamental freedoms as enshrined in EU law.

In 2016 (i.e., also after *Schrems I*, but more importantly also after the Snowden revelations), the Article 29 Working Party issued a working document "*on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)*,"[9] in which it sets out crucially important standards in that regard.

In the CJEU's *Schrems II* judgment (that we discuss Part Two), the surveillance regime of the USA was assessed with reference to EU fundamental rights standards, and found wanting.

[7] Hansard, 8 September 2020, volume 679, column 509, available at: https://www.theguardian.com/law/2020/sep/13/uk-government-plans-to-remove-key-human-rights-protections

[8] *UK government plans to remove key human rights protections*, Observer/Guardian, 13 September 2020, available at: https://www.theguardian.com/law/2020/sep/13/uk-government-plans-to-remove-key-human-rights-protections More recently, the Government has appeared to be rowing back from this threat, but it – and many Conservative MPs – remain hostile to the Convention. See: *Boris Johnson set for compromise on Human Rights Act – EU sources*, Guardian, 7 October 2020, available at: https://www.theguardian.com/politics/2020/oct/07/boris-johnson-set-to-make-compromise-on-human-rights-act-eu-sources

[9] WP29, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (WP237), adopted on 13 April 2016, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640363
This document was not endorsed by the EDPB, presumably because it was a working document on an issue on which the Board itself wanted to reflect further and because *Schrems II* was still pending.

2.1.3 Implications in relation to the UK

As we shall see in Part Two, two legal regimes relating to access to personal data by the UK national security agencies have been held to violate Article 8 of the European Convention on Human Rights in the *Big Brother Watch* judgment of the European Court of Human Rights. It follows that, if applied to EU data, they also fail to meet fundamental requirements of EU fundamental rights law. A third regime was held to be compatible with the ECHR – but only because of an approach taken by the Strasbourg Court that is not adopted by the Court of Justice in Luxembourg.

We will show, with reference to *Schrems II* and a series of other CJEU judgments, that that latter legal regime, and some other regimes that were not assessed by the ECtHR, do not limit access by the UK's national security agencies to personal data – including data that may have been transferred from the EU to the UK, or that may be accessible by them from the UK – in a way that is compatible with the EU standards, as set in those cases and in the WP29 "Essential European Guarantees".

That too stands in the way of a UK adequacy decision.

2.1.4 The issue of "onward transfers"

One related important matter is the question of "onward transfers" of personal data that have been exported from the EU to a country held to provide adequate/essentially equivalent protection, to another third country that has not been so declared (and, where the adequacy decision is limited to a particular sector or category of recipients in the first "third country", also to any recipient in that first third country who is not covered by that decision). As we have seen, Article 44 GDPR now stipulates expressly that transfers of personal data that are subject to that instrument, "*including onward transfers*" of such data, may only take place if it is ensured that the conditions set out in the GDPR are complied with, and more generally, that "*the level of protection of natural persons guaranteed by this Regulation is not undermined*."

This means that third countries cannot be held to provide adequate/essentially equivalent protection to personal data as is provided by the GDPR in the EU, unless their domestic law ensures not only such protection domestically, but also ensures that protection continues if personal data imported from the EU are further, "onwardly" transferred to another country or recipient that is not covered by the adequacy decision.

Although this was already formally the position in 2011,[10] the issue has only recently been taken seriously. In most older adequacy decisions, this issue was barely addressed: the words "onward transfer" do not appear at all in the adequacy decisions on Switzerland (2000),

[10] The 1998 WP29 working document on transfers of personal data to third countries (WP12, footnote 6, above) already stipulated under the heading "Restrictions on onward transfers" that: "*[F]urther transfers of the [exported] personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive [i.e., with the provision on transfers based on 'appropriate safeguards' such as SCCs, now Article 46 GDPR]*".

Canada (2001),[11] Argentina (2003), Guernsey (2003), Isle of Man (2004), Jersey (2008), Andorra (2010), the Faroe Islands (2010), New Zealand (2012) and Uruguay (2012).[12]

In the 2011 adequacy decision on Israel, there is a stipulation in recital (14) that:

> Further onward transfers to a recipient outside the State of Israel, as defined in accordance with international law, should be considered as transfers of personal data to a third country –

but the implications are not spelled out (even though they are significant).

On the other hand, the two adequacy decisions on the USA (both now invalidated) did set out clear restrictions on onward transfers. As it was put in the latest of them, dating from 2016:[13]

> **Special rules apply for so-called 'onward transfers', i.e. transfers of personal data from an organisation to a third party controller or processor, irrespective of whether the latter is located in the United States or a third country outside the United States (and the Union). The purpose of these rules is to ensure that the protections guaranteed to the personal data of EU data subjects will not be undermined, and cannot be circumvented, by passing them on to third parties.** This is particularly relevant in more complex processing chains which are typical for today's digital economy.
>
> Under the *Accountability for Onward Transfer Principle*, any onward transfer can only take place (i) for limited and specified purposes, (ii) on the basis of a contract (or comparable arrangement within a corporate group) and (iii) only if that contract provides **the same level of protection as the one guaranteed by [the EU-US Privacy Shield Principles]**, which includes the requirement that the application of the Principles may only be limited to the extent necessary to meet national security, law enforcement and other public interest purposes. …
>
> *(recitals (27) – (28), notes omitted, original italics, emphasis in bold added)*

The EU-US Privacy Shield Decision may have been invalidated – but the above principle still stands and is indeed reinforced under the GDPR. This is made clear in the latest adequacy decision, on Japan,[14] issued in 2019 (the first to be issued under the GDPR). This has a whole section on onward transfers, section 2.3.9, that stipulates in its first paragraph (para. 75 in the decision) that:

> The level of protection afforded to personal data transferred from the European Union to business operators in Japan must not be undermined by the further transfer of such data to recipients in a third country outside Japan. Such "onward transfers", which from the perspective of the Japanese business operator constitute

[11] The WP29 Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act, adopted on 26th January 2001 (WP39), does raise issues in this regard: see the section on *Interaction with Provincial legislation and Onward transfers* on pp. 5 – 6, but this is not reflected in the Commission Decision.

[12] Links to all these adequacy decisions can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[13] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:TOC

[14] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC

> international transfers from Japan, should be permitted only where the further recipient outside Japan is itself subject to rules ensuring **a similar level of protection as guaranteed within the Japanese legal order**.
>
> (emphasis added)

In the light of the *Schrems I* judgment, in any future adequacy decisions, references such as those in the Privacy Shield Decision to "*the same level of protection as the one guaranteed by [the EU-US Privacy Shield Principles]*" and in the Adequacy Decision on Japan to "*a similar level of protection as guaranteed within the Japanese legal order*" should be replaced by a clear and explicit requirement that the onwardly forwarded data should be subject to protection at a level that is "*essentially equivalent to that provided by EU law*" – otherwise, that high EU level could still be undermined by onward transfers. Moreover, as we shall see in section 3.3 below, if that level of protection cannot be guaranteed in relation to to-be-onwardly transferred data, the onward transfer would be in violation of the GDPR.

The European data protection authorities now also stress that compliance in this respect lies squarely with the parties to the transfer, in particular the recipient in the third county to which the data were originally transferred from the EU:[15]

> **Restrictions on onward transfers**
>
> Further transfers of the personal data by the initial recipient of the original data transfer should be permitted only where the further recipient (i.e. the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller. **The level of protection of natural persons whose data is transferred must not be undermined by the onward transfer. The initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision.** Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing.
>
> (emphasis added)

In other words, onward transfers of personal data from a country that has been held to provide adequate/essentially equivalent protection of such data (compared to the EU) to another third country that has not been held to provide such protection (or to a recipient in the first third country that is not covered by the EU adequacy decision) should only be allowed under contractual or similar arrangements that ensure that the recipient is subject to rules that ensure continued protection for the EU data at a level that is "essentially equivalent" to that accorded by the GDPR; otherwise, there would still be room for undermining of the EU rules. This includes the question of whether the state agencies in the second third country or territory may obtain undue access to the onwardly transferred data.

[15] WP29, Adequacy Referential (footnote 6, above), section A.9, on p. 3.

Stipulations on the lines of the USA and Japan onward transfer ones (but explicitly referring to the need for "essential equivalence" rather than using weaker terms) will now have to be included in any EU adequacy decision. Onwardly transferred data must be protected against undue (indiscriminate, not strictly necessary or disproportionate) access by the authorities in the second third country (just as they have to be protected against such undue access by the authorities in the first third country).

A further major point to be made in this regard is that the question of whether the other third country or the recipient in the first third country is subject to "rules ensuring a similar/adequate/essentially equivalent level of protection" to the EU is a matter for the EU to determine. The European Commission and the EU Member States' supervisory authorities are required to keep this issue under continuous review, and must intervene if they feel personal data sent from the EU to a country that has been held to provide adequate protection are at risk of losing the EU level of protection by disclosures to the first third country's agencies, or by onward transfers to other third countries.

2.1.5 Implications in relation to the UK

The "onward transfer" issue is of particular importance in relation to the new legal regime in the UK after the post-Brexit transition period, when the "UK GDPR" will come into force in the UK, replacing the EU GDPR that applies until then. The UK GDPR is modelled on the EU GDPR (albeit, as we shall explain in section 3, with a number of serious deficiencies).[16]

Here, we should note the UK GDPR also mirrors the EU GDPR in relation to the approach to transfers to other countries. The UK wants to offer the Union a UK adequacy decision (taken under sections 17A to 17C of the UK GDPR) in return for an EU decision to the effect that UK law is adequate in terms of (i.e., ensures essentially equivalent protection to) the EU GDPR.

But in relation to other countries, the UK wants to assert its own – in its own view, restored – full sovereignty: the UK GDPR grants the UK authorities the independent right to declare that other countries (and territories) provide adequate protection in its own terms. The UK will certainly declare the Channel Islands and the Isle of Man to provide adequate protection – which would become problematic if the EU were to rescind its adequacy decisions in relation to those territories (as we will suggest it should do in the light of the application of UK surveillance law there). The UK's Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations already specify that Gibraltar provides adequate protection (in terms of the UK GDPR) even though the Commission has not ever issued a positive adequacy decision in relation to that territory.

Serious concerns also arise in relation to the agreement between the UK and the USA on access to electronic data for the purpose of countering serious crime.[17] Under this Agreement,

[16] The text of the modifications to the (EU) GDPR and to the UK Data Protection Act 2018 (that applied the (EU) GDPR in the UK and spelled out the further specifications that the latter left to Member States), to form the UK GDPR is available at: https://www.gov.uk/government/publications/data-protection-law-eu-exit

[17] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington DC, USA, 3 October 2019 (not yet in force), available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

once it comes into force, data including e-communications data, also of EU persons (which are subject to the GDPR and the e-Privacy Directive), will be made available to U.S. agencies, under rules that we believe do not meet the onward transfer requirements of the GDPR. Article 3(3) of the Agreement stipulates:

> Each Party in executing this Agreement recognizes that the domestic law of the other Party, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities subject to this Agreement.

The UK and the USA therefore effectively agree to order their domestic companies holding any electronic data to hand over such data to the other country's law enforcement agencies on the basis of orders issued under the latter country's laws.

Given neither the First Amendment to the U.S. Constitution, covering free speech and freedom of association, nor the Fourth Amendment, protecting citizens from "unreasonable searches", apply to "non-US persons" (I.e., individuals who are neither citizens of nor lawful residents in the USA), we have serious reservations in that regard.[18]

Moreover, in our view, the UK is also highly likely (to facilitate a free trade deal) to declare the USA provides adequate protection to personal data in UK GDPR terms – even though the CJEU has now twice ruled (in *Schrems I* and *II*) it does not.

What is more, as we shall show in Part Two, the UK and the USA share effectively all intelligence data under the so-called UKUSA Agreement, (along with Canada, Australia and New Zealand), and this will undoubtedly continue after 2020.

All these matters raise serious concerns about the effect of an EU positive adequacy decision on the UK. If the EU were to grant the UK a positive adequacy decision, personal data on EU individuals could be freely transferred to the UK. But if the UK were to then declare, under its "UK GDPR", the USA is deemed to provide adequate protection, personal data transferred from the EU to the UK could freely be further transferred ("onwardly transferred") without further ado to the USA.

That would open an obvious means of evading the EU restrictions on transfers of personal data to the USA.

[18] Cf. Respectively, as regards the First Amendment:
"[T]he interests in free speech and freedom of association of foreign nationals acting outside the borders, jurisdiction, and control of the United States do not fall within the interests protected by the First Amendment" (*DKT Memorial Fund Ltd. v. Agency for International Development*, 1989, quoted in *Chevron Corporation v. Steven Donziger et al*., US District Judge Kaplan order of 25 June 2013).
The Fourth Amendment similarly does not apply if the person affected by a "search" (which includes online searches) has no "significant voluntary connection with the United States": *US v. Verdugo-Urquidez*, 1979. This was confirmed to the EU-US Working Group on Data Protection, set up to investigate the US surveillance activities exposed by Snowden: see Report on the Findings by the EU Co-chairs of the Ad hoc EU-US Working Group on Data Protection, 27 November 2013, section 2, para. 2.

In simple terms: granting the UK a positive adequacy decision without addressing the requirements for a UK Government-issued adequacy decision on other third countries would directly undermine the protection of personal data in the EU. And this applies both in relation to transfers of commercial data subject to the GDPR, such as e-communications data, passenger name records, etc., by commercial entities, and to transfers of personal data relating to EU individuals, obtained by the UK national security agencies under the contentious regimes already mentioned, to U.S. (and other) intelligence partners of the UK.

2.2 The process for adopting an adequacy decision

A Commission adequacy decision must be adopted in a "comitology" process, set out in the EU Comitology Regulation, Regulation (EU) No 182/2011 (Article 93 GDPR), but with some special features. Basically, the Commission (in practice, the Directorate-General for Justice and Consumers, "DG JUST" and more specifically its International Data Flows and Protection Unit, JUST.C.4) is charged with drafting the decision, but must, under the GDPR, consult the European Data Protection Board, which must issue an opinion on whether the third country in question provides adequate protection (Article 70(1)(s) GDPR). In order to facilitate this work by the EDPB:

> the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation. (*idem*)

The Commission is not bound by the EDPB opinion – but it would be difficult for it to issue a positive adequacy decision on the UK in the face of a considered opinion by the most expert EU body in this field that the UK does not provide adequate protection.

The draft decision must be submitted to the "Article 93 Committee", made up of representatives of the EU Member States, for approval by consensus or by qualified majority. If the Article 93 Committee approves a delegated act, the Commission must adopt the act.

At the same time, the Commission must make the draft decision available to the European Parliament and the Council.[19] As Kuner points out:[20]

> The Parliament and the Council are normally not involved in preparation of implementing acts and do not participate in meetings of the Article 93 Committee. They can neither block the adoption of a draft implementing act nor 'call back' the implementing powers. However, at any stage of the procedure, the Parliament or the Council may indicate to the Commission that, in its view, a draft implementing act exceeds the implementing powers provided for in the GDPR. In such a case, the Commission must review the draft and inform the other institutions whether it intends to maintain, amend or withdraw it.

Parliament also has the power to refer a decision that has been adopted to the Court of Justice for annulment, if it feels the decision is in breach of the Treaties or the Charter of Fundamental Rights. And, as seen in the two *Schrems* cases, data protection authorities can also, of their own accord or at the behest of individual data subjects, refer questionable adequacy decisions to the Luxembourg Court, via their domestic courts – and are indeed, in the Luxembourg Court's *Schrems II* judgment (further discussed in Part Two), again expressly

[19] See Article 10(5) Comitology Regulation.

[20] Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds) and Laura Drechsler (Asst Ed.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, 2020, commentary on Article 93, section 2, *The procedure for implementing acts*, footnotes omitted.

invited to do so in appropriate cases (although pending such litigation the decision remains in force):[21]

> even if the Commission has adopted a Commission adequacy decision, the competent national supervisory authority, when a complaint is lodged by a person concerning the protection of his or her rights and freedoms in regard to the processing of personal data relating to him or her, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the GDPR and, where relevant, to bring an action before the national courts in order for them, if they share the doubts of that supervisory authority as to the validity of the Commission adequacy decision, to make a reference for a preliminary ruling for the purpose of examining its validity
>
> (*Schrems II* judgment, para. 120)

Put simply: a positive adequacy decision should only be issued when the assessment of the third country on which it rests (in relation to all of the earlier-mentioned elements) is sound; they should not be issued for political reasons or to facilitate trade, when adequate protection is not ensured in the third country. The invalidations of the EU-US Safe Harbour and Privacy Shield Agreements by the Court are stark reminders of that.

This submission is sent to all the above-mentioned bodies involved in adequacy decisions: the Commission (Unit JUST.C.4), the EDPB, the Article 93 Committee and the European Parliament (LIBE Committee) in the hope it will be helpful to their deliberations.

2.3 Keeping adequacy decisions under review

Under the GDPR, the Commission must not only **review** every adequacy decision it issues every three years (Article 45(3)), but in addition, it must "*on an ongoing basis, **monitor developments***" in third countries that have been granted an adequacy decision (Article 45(4), emphasis added) and it must **repeal, amend or suspend** the decision if "*information reveals … that a third country … no longer ensures an adequate level of protection*" (Article 45(5)).

The EU Member States' supervisory authorities may also suspend data flows to third countries held to provide adequate protection if it transpires that this is not ensured any longer.[22]

However, these powers have never been exercised in practice.

- o – O – o -

[21] The Court had already pointed this way in its earlier *Schrems I* judgment.

[22] See the standard clause to that effect, included *verbatim* in the adequacy decisions on Canada (2001, Article 3), Argentina (2003, Article 3), Andorra (2010, Article 3), Israel (2011, Article 3) and in less explicit terms in the adequacy decisions on the USA (2016 – the now invalidated Privacy Shield decision, Article 3 and 4(3)) and Japan (2019, Article 2 and 3(3)).

3. Inadequacy of UK data protection law after the post-Brexit transition period

3.1 Introduction

The UK initially contemplated a special EU-UK data agreement in the form of a bilateral treaty encompassing mutual recognition of data protection standards. The UK also wanted "a continued role" for the UK data protection authority, the Information Commissioner's Office (ICO), in the European Data Protection Board (preferably membership), as well as UK participation in the One-Stop-Shop, which it felt would be good for UK businesses.[23]

Presumably, the reason for initially aiming for a treaty arrangement rather than an adequacy decision was that under international law a treaty cannot be unilaterally disapplied, while an adequacy decision can be unilaterally repealed, amended or suspended by the EU – and must be "*where available information reveals … that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection*" (Article 45(5) GDPR).[24]

However, the UK Government subsequently abandoned its aim of a special treaty and, on 20 January 2020, issued a statement expressing its intention "to secure adequacy decisions from the European Commission to enable personal data to continue to flow freely from the European Union to the United Kingdom and Gibraltar".[25] On 13 March, it released a:[26]

> comprehensive pack of explanatory material [that] provides an overview of the United Kingdom's legal framework underpinning high data protection standards in order to assist the European Commission in conducting its assessment.

That framework will consist mainly of the "UK GDPR" and related UK law as it will be applied after the transition period.[27] As already briefly noted, that "UK GDPR" is largely modelled on the EU GDPR – but also modifies it in some respects. Moreover, its application is affected by

---

[23] See: HM Government, *Technical Note: Benefits of a new data protection agreement*, 2018, p. 1, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714677/Data_Protection_Technical_Note.pdf
For further details, see Oliver Patel and Dr Nathan Lea, EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?, UCL European Institute, August 2019, p. 8, available at: https://www.ucl.ac.uk/european-institute/sites/european-institute/files/eu-uk_data_flows_brexit_and_no_deal_updated.pdf

[24] This is of course rather ironic in view of the recent decision of the UK Government to give itself statutory powers to deliberately unilaterally break its international legal obligations under the Withdrawal Agreement (an international treaty), in acknowledged violation of its treaty obligations under international law. See footnote 7, above.

[25] The reference to Gibraltar is interesting. The information pack referenced in the next footnote contains a special section (Section I, consisting of four separate sub-sections) on Gibraltar, suggesting the territory should be regarded as providing adequate protection (essentially, because it follows UK data protection law). But unlike the Channel Islands and the Isle of Man, the EU never adopted a positive adequacy decision on Gibraltar. We will return to this in Part Two.

[26] The UK's Explanatory Framework for Adequacy Discussions pack is available in sections from this government website: https://www.gov.uk/government/publications/explanatory-framework-for-adequacy-discussions#:~:text=The%20United%20Kingdom%20is%20seeking,and%20United%20Kingdom%20and%20Gibraltar.

[27] The "UK GDPR" as it will come into effect on 1 January 2021 consists of the (EU) GDPR as applied in the UK prior to that date (also referred to as the "UK GDPR") and the 2018 UK Data Protection Act that further specified various matters that the GDPR left to EU Member States to regulate in detail, as both amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, which are available here:
https://www.legislation.gov.uk/ukdsi/2019/9780111177594/pdfs/ukdsi_9780111177594_en.pdf

a number of other factors. We will note below some major deficiencies in relation to the "core" substantive requirements of EU data protection law, potential divergence, and "procedural/enforcement" guarantees, before turning to UK surveillance laws and practices in Part Two.

3.2 Deficiencies in the "core" substantive requirements of post-Brexit data protection regime

3.2.1 The Digital Economy Act 2017 and its data sharing provisions

Despite its modification by the UK's Data Protection Act 2018, the **Digital Economy Act 2017** appears to allow for wide sharing of superficially de-identified data, subject to fewer restrictions than provided for in the (EU) GDPR.

The GDPR makes clear that data should be treated as "personal data" if the data subject can be "singled out" (be that by the controller or by another person: Recital 26). "Singling out" of an individual need not involve the revelation of that person's identity: information such as, say, a photograph of a person who is labelled a "suspected shoplifter" (thief) must be regarded as personal information under the GDPR, even if that person's name or other identifying particulars are not known. Similarly, processing of pseudonymised data by a recipient who has no access to the pseudonymisation "key" but who may be able to "single out" the individual (or even identify her by name) from other data must be treated as personal data.

By contrast, the DEA stipulates that in relation to public service delivery:

> information identifies a particular person if the **identity** of that person—
>
> (a) is specified in the information,
>
> (b) can be deduced from the information, or
>
> (c) can be deduced from the information taken together with any other information.
>
> (DEA, section 40(6), emphasis added)

This suggests that while data on unidentifiable[28] but singled-out individuals must, under the (EU) GDPR, be treated as personal (identifiable) data, and can therefore only be shared subject to the various conditions for processing (legal basis/specifically authorised in a [clear and foreseeable] law that "respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" to safeguard major public interests [Article 23]; purpose limitation; data quality, minimisation and relevance; etc.),

[28] We believe this reading of Article 40(6) DEA is not affected by the stipulation in Article 40(8) that "nothing in sections 35 to 39 authorises the making of a disclosure which— (a)contravenes the data protection legislation". The latter term is defined in the DPA2018 as covering "the GDPR, the applied GDPR, this Act 9 [the DPA2018], regulations made under this Act, and regulations made under section 2(2) of the European Communities Act 1972 which relate to the GDPR or the Law Enforcement Directive." (DPA2018, section 3(9)). However, from 1 January 2021, the term will cover only UK data protection law, and while, for the time being, the "UK GDPR" still retains the definition of "personal data" as set out in Article 4(1) of the (EU) GDPR, it does not contain the clarification contained in Recital 26 of the (EU) GDPR about "singling out" of a person or identification "by the controller or another person". Moreover, from that date the UK courts will no longer be required to apply the term "personal data" broadly, but can apply it more restrictively, in line with the DEA. In any case, the UK Government could if needs be amend the law by ministerial order if it felt the courts were interpreting the term too broadly: see section 3.3.1, below.

under the UK DEA – and the UK GDPR – data can be much more widely shared and used.[29] This will also apply to personal data transferred to the UK after the post-Brexit transition period (irrespective of whether they are transferred in identifiable or pseudonymised form). This "generous" approach to data sharing fits in with the UK government's declared aim to make the widest possible use of personal data, especially in the public and quasi-public sectors.

Interestingly, although there are repeated references to the "digital economy" in one of the UK Government's documents, on the "wider context",[30] the Digital Economy Act is not mentioned in the main documents.[31]

3.2.2 The "immigration exemption"

Other specific serious concerns have been raised about the so-called **"immigration exemption"** in the UK data protection legislation that directly affects all EU citizens resident in the UK. Paragraph 4(1) in Part 1 of Schedule 2 to the DPA2018 stipulates:

> The GDPR provisions listed in sub-paragraph (2) do not apply to personal data processed for any of the following purposes—
>
> (a) the maintenance of effective immigration control, or the maintenance of effective immigration control, or
>
> (b) the investigation or detection of activities that would undermine the maintenance of effective immigration control, the investigation or detection of activities that would undermine the maintenance of effective immigration control,
>
> to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) and (b).

The "GDPR provisions" in question, which do not apply to processing for immigration purposes, are those guaranteeing the rights of data subjects to be informed of processing of their data, to obtain confirmation of processing and access to their data, as well as their rights

[29] We believe that this reading of Article 40(6) DEA is not affected by the stipulation in Article 40(8) that "nothing in sections 35 to 39 authorises the making of a disclosure which— (a)contravenes the data protection legislation". The latter term is defined in the DPA2018 as covering "the GDPR, the applied GDPR, this Act 9 [the DPA2018], regulations made under this Act, and regulations made under section 2(2) of the European Communities Act 1972 which relate to the GDPR or the Law Enforcement Directive." (DPA2018, section 3(9)). However, from 1 January 2021, the term will cover only UK data protection law, and while, for the time being, the "UK GDPR" still retains the definition of "personal data" as set out in Article 4(1) of the (EU) GDPR, it does not contain the clarification contained in Recital 26 of the (EU) GDPR about "singling out" of a person or identification "by the controller or another person". Moreover, from that date the UK courts will no longer be required to apply the term "personal data" broadly, but can apply it more restrictively, in line with the DEA. In any case, the UK Government could amend the law by ministerial order if it felt the courts were interpreting the term too broadly: see section 3.3.1, below.

[30] HMG, Explanatory Framework for Adequacy Discussions (footnote 26, above), *Section B: Wider Context*.

[31] *Idem*, *Section C: The UK's Legislative Framework* and *Section D: Adequacy Referential*. It is also reminiscent of the inadequate definition of "personal data" in the 1984 UK Data Protection Act, which did not include the clarification that data should be regarded as "identifiable" if they can be linked to an individual *by the controller or by another person*. The European Commission found this to be in violation of the 1995 Data Protection Directive and threatened legal action – but in the end did not pursue it further.

to erasure, objection and restriction of processing, as well as safeguards for third country transfers (para. 4(2)(a) - (f)).

Even the most fundamental general data protection principles, set out in Article 5 of the UK GDPR (corresponding to Article 5 of the (EU) GDPR, at least for the time being) – such as the principles that personal data must be processed lawfully and fairly and for a specific, specified purpose and not use for incompatible purposes – do not apply to processing of personal data for immigration purposes, "[in] so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (a) to (f)" (para. 4(2)(g)).

Of course, if information and access to one's file is denied, one can also not effectively exercise one's rights to correct incorrect data; and in any case the rights to object and restrict contested data are removed. And that in turn fundamentally affects one's rights to fair proceedings in immigration cases, including in cases relating to the rights of EU nationals. Paragraph 4, sub-clauses (3) and (4), also removes restrictions on sharing of data between bodies – a long-standing issue in the UK, what the UK campaign group *Open Rights Group* (ORG) calls "a shadowy, opaque, pernicious problem".[32]

This again fails to be "essentially equivalent" to the GDPR in that such exemptions must be based on clear and foreseeable legal rules that "respect[] the essence of the fundamental rights and freedoms and [are] a necessary and proportionate measure in a democratic society" to safeguard major public interests (Article 23).

ORG and *the3million*, an NGO campaigning for the rights of EU nationals in the UK,[33] challenged the immigration exemption in the UK High Court. With reference to the "Windrush" scandal in which many UK immigrants of Caribbean origin had been appallingly treated over many years, they argued the law was too vague and broad and allowed for subjective, arbitrary denial of data subjects' rights. However, their challenge was rejected.

Interestingly, the UK data protection supervisory authority, the Information Commissioner's Office (ICO), intervened to argue the exemption would only be lawful if accompanied by statutory guidance on its use. However, the High Court found "*the provisions of the exemption setting out the purposes for which, and the categories of data to which, it may be applied are, in my view, clear and appropriately delineate*", and "*a legislative measure does not require to be accompanied by guidance as to proportionality in order to be lawful*".[34]

Rosa Curling of Leigh Day (which represented *the3million*) commented:[35]

> millions of people are already feeling uncertain and anxious about their immigration status as we approach Brexit and our clients feel that the immigration exemption adds a further layer of uncertainty by removing transparency and the opportunity to correct mistakes in the immigration system.

[32] Open Rights Group, *what is at stake with the immigration exemption legal challenge?*, 3 August 2018, available at: https://www.openrightsgroup.org/blog/what-is-at-stake-with-the-immigration-exemption-legal-challenge/

[33] See: https://www.the3million.org.uk/

[34] *R (Open Rights Group & the3million) v Secretary of State for the Home Department [2019] EWHC 2562 (Admin)*, 3 October 2019, available at: https://www.bailii.org/ew/cases/EWHC/Admin/2019/2562.html

[35] See: https://www.freemovement.org.uk/high-court-upholds-immigration-control-exemption-to-personal-data-rights/

The NGOs are seeking permission to appeal to the Court of Appeal,[36] but even if this is granted, no final decision is expected before the end of the post-Brexit transition period, which ends on 31 December 2020.

Again interestingly, none of the just-mentioned UK Government documents (Sections A, B and C)[37] make any mention of this exemption (or indeed of immigration).

In our view, the UK cannot be granted a positive adequacy decision unless the definition of "personal data" in the Digital Economy Act is brought into line with the definition of that term in the (EU) GDPR, and unless the application of the immigration exemption in the Data Protection Act is significantly tightened, made clear and foreseeable in its application, and is limited to what is objectively necessary and proportionate in a democratic society.

NB: It might well have been possible to smooth out these *prima facie* deficiencies in UK law through interpretations consistent with EU law including the GDPR and the CFR by the UK courts, and if needed be by the CJEU, as would have been the case if the UK was still a Member State of the EU. But of course, the whole point of Brexit is that the UK is no longer an EU Member State and, from 1 January 2021, will no longer be obliged to keep its laws in line with EU law in relevant areas, and in such areas apply or interpret its domestic law in accordance with EU law. On the contrary, as discussed next, unless restrained by any future EU-UK treaty, the UK will be able to diverge in its laws and their application and interpretation from the laws and interpretations of the EU – and it is clearly intent on doing exactly that. It is not even certain it would adhere to any future treaty constraints in this respect. This means the above-mentioned issues will then come to the fore, as can any number of other issues.

3.3 Probable future divergence

3.3.1 Divergent data protection law

Apart from the already-noticeable deficiencies in the post-Brexit UK data protection regime, discussed above, there is also the wider issue of – highly probable, and indeed expressly intended – **future divergence**. Specifically, the UK's European Union (Withdrawal) Act (WA) allows for modifications to the "UK GDPR" after transition across any article by ministerial order. As Chris Pounder pointed out last year, even if that instrument may appear at first glance to be (almost) identical to the actual (EU) GDPR, the WA provisions allow a "coach and horse" to be driven through it at any time afterwards.[38]

In a later post, Pounder noted that the Prime Minister, Boris Johnson, clearly signalled that he is prepared, if needed, for the UK to depart from EU norms of data protection. Johnson

[36] ORG, *Open Rights Group and the3million seek to appeal immigration exemption judgment*, 3 October 2019, available at: https://www.openrightsgroup.org/press-releases/open-rights-group-and-the3million-seek-to-appeal-immigration-exemption-judgment/

[37] See footnotes 30 and 31, above. Both can be found in the link in footnote 26.

[38] See Chris Pounder, *Draft Brexit Data Protection Regulations would undermine adequacy determination for the UK*, 18 January 2019, available at: https://amberhawk.typepad.com/amberhawk/2019/01/draft-brexit-data-protection-regulations-would-undermine-adequacy-determination-for-the-uk.html (see under "*Powers to diverge differ*")

said: "*We will restore full sovereign control over our borders and immigration, competition and subsidy rules, procurement and* ***data protection***" (Pounder's emphasis).[39]

Pounder adds, rightly, that "*in effect, any adequacy agreement between the UK and European Commission will have to contain a guarantee, given by the UK Government, concerning permitted divergence between the UK_GDPR from the GDPR. For example, with respect of further disclosure to public bodies or that any change to, rights, principles and other GDPR obligations does not deviate too far from European norms."* But he also rightly adds that *"For the life of me, I cannot see such a guarantee being given if the Government's mantra of 'taking back control' is to be realised."*[40]

Rather, the UK Government, spurred on by the UK prime minister's deliberately "disruptive" senior adviser, Dominic Cummings, is proposing "an overhaul in the use of data across the public sector" under a new "National Data Strategy" where:

> data and data use are seen as opportunities to be embraced, rather than threats against which to be guarded.
>
> This means asking fundamental questions about what data should and should not be made available across the UK. It means maintaining a regulatory regime that is not overly burdensome for smaller businesses and that supports responsible innovation. It means driving a radical transformation of how the government understands and unlocks the value of its own data to improve a range of public services and inform decisions[41]

In this context, (as the EU has apparently noted), the UK Government appears to want "to rewrite Britain's data protection laws" after transition.[42]

These intentions are linked to the desire of the UK Government to open up free trade with the rest of the world (especially outside the EU), with free data flows. To this end, it has included provisions in various pending Free Trade Agreement (FTAs).[43] This is in direct contrast to the EU policy under which personal data may not be included in FTAs.[44]

---

[39] See Chris Pounder, *Adequacy of the UK's data protection regime; now the UK has left the EU, the battle lines are drawn*, 3 February 2020, available at: https://amberhawk.typepad.com/amberhawk/2020/02/adequacy-of-the-uks-data-protection-regime-now-the-uk-has-left-the-eu-the-battle-lines-are-drawn.html

[40] *Idem*. See also Oliver Patel and Dr Nathan Lea, EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray? (footnote 12, above) who also broadly concur with us on the negative implications of the UK surveillance regime for any adequacy decision (as does Pounder). Those implications are discussed in Part Two.

[41] UK Government, National Data Strategy, 9 September 2020, available at: https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#ministerial-foreword

[42] See: *Dominic Cummings' data law shake-up a danger to trade, says EU*, Guardian, 25 September 2020, available at: https://www.theguardian.com/politics/2020/sep/25/dominic-cummings-data-law-shake-up-a-danger-to-trade-says-eu See also *Data protection on course to become the most contested issue in EU/UK relations*, Eurointelligence, 28 September 2020, available at: https://www.eurointelligence.com/ ($)

[43] Open Rights Group, forthcoming.

[44] Cf. the European Parliament resolution of 12 December 2017 "*Towards a digital trade strategy*" (2017/2065(INI)), Section V, in which it stressed that "*The protection of personal data is non-negotiable in [EU] trade agreements*", available at: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_EN.pdf This is reflected in the European Commission set of "*horizontal provisions for cross-border data flows and for personal data protection (in EU trade and investment agreements)*", adopted on 31 January 2018 and leaked on the Politico website at: https://www.politico.eu/wp-content/uploads/2018/02/Data-flow-provisions-POLITICO.pdf

If the UK were to be granted a positive adequacy decision, and were then to include such clauses in the UK-USA FTA it is strenuously aiming for, that would open up a further route by which personal data transferred from the EU to the UK without impediments (because of that adequacy decision) could be onwardly transferred to the USA, in spite of the ruling in the CJEU's *Schrems II* judgment the USA does not ensure adequate/essentially equivalent protection because of its surveillance regime.

3.3.2 Diverging from European fundamental rights standards

The UK Government has been extremely clear it wants to free itself from the "shackles" of the EU Charter of Fundamental Rights and the oversight of the Court of Justice of the European Union. In fact, it sees that as one of the great gains of Brexit.

But even more broadly, the UK Government has indicated it wants to be able to "opt out" of parts of the European Convention on Human Rights, at least from the interpretations of the Convention by the European Court of Human Rights.[45] The latter would be in line with the UK Government's express willingness to take action against what it perceives as judicial "overreach" domestically.[46]

Consequently, the government "is resisting giving Brussels a formal undertaking to adhere to the Convention." *The Observer* quotes a government spokesperson as saying:[47]

> The UK is committed to the European convention on human rights and to protecting human rights and championing them at home and abroad, but we believe that this does not require an additional binding international legal commitment.
>
> **How the UK gives effect to its longstanding strong human rights protections is a matter for the UK as an autonomous country. In the same way, it's a matter for the EU and its member states to give effect to their own human rights protections according to their own legal orders.** (emphasis added)

In theory, the European Commission and the EU Member States' supervisory authorities can intervene if they were to notice in future that the UK had diverged from the "essentially equivalent" standard: see section 2.3, above. However, as noted there, in practice this has never been done.

[45] *UK government plans to remove key human rights protections*, Observer/Guardian, 13 September 2020, available at: https://www.theguardian.com/law/2020/sep/13/uk-government-plans-to-remove-key-human-rights-protections

[46] *Idem*. Specifically, domestically, a panel under a former Tory justice minister, Lord Faulks, is looking at curbing the powers of judges to intervene in what it argues are political decisions. See: *The UK's reputation for rule of law is in jeopardy*, Financial Times, 9 September 2020, available at: https://www.ft.com/content/351fe714-cc87-4b36-8562-fcd3533fff45

[47] *UK government plans to remove key human rights protections*, Guardian/Observer, 13 September 2020, emphasis added, available at: https://www.theguardian.com/law/2020/sep/13/uk-government-plans-to-remove-key-human-rights-protections

We believe there are not only serious doubts as to whether the UK can be granted a positive adequacy decision (see section 3.2, above), but especially grave reservations as to whether the UK would continue to ensure protection to personal data that is "essentially equivalent" to the EU level in future. A positive decision should certainly not be granted without clear, binding commitments on the part of the UK to not diverge substantially from the EU standards in future. Without a legal commitment to that effect, in a binding treaty, future compliance with EU standards cannot be assumed (and regrettably, given the situation with the Internal Market Bill, noted earlier,[48] there are even doubts as to whether the UK would comply with its international obligations under such a treaty).

3.4 Deficiencies in the "procedural/enforcement" guarantees in the post-Brexit data protection regime

On "procedural/enforcement" matters, it should be noted that although the UK data protection supervisory authority, the ICO, is one of the largest in Europe, it has been severely criticised for not effectively enforcing the law, both in terms of its minimum application of sanctions and in terms of its lack of real support for data subjects that bring complaints.[49] It appears to have largely given up on enforcing the law during the coronavirus pandemic.[50]

Moreover, there are major, long-standing questions about its independence, which are also reinforced by differences between the (EU) GDPR and the "UK GDPR". As explained by Chris Pounder:[51]

> **Independence of the Commissioner?**
>
> The modified Article 52 [in the "UK GDPR"] still allows the ICO independence of action; however, the ICO is not wholly independent. Consider changes proposed by Regulation 45(3) [of the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 that brought the "UK GDPR" into law] which says:
>
> > In paragraph 1 (of Article 51) —
> >
> > (a) for "*Each Member State shall provide for one or more independent public authorities to be*" substitute "*The Commissioner is*";
> >
> > (b) omit "*within the Union ("supervisory authority")*".
>
> Applying the above changes, Article 51(1) of the GDPR becomes:
>
> > 51(1). ~~Each Member State shall provide for one or more independent public authorities to be~~ [*The Commissioner is*] responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

[48] See footnote 7, above.

[49] *If ICO won't regulate the law, it must reboot itself*, Information Rights and Wrongs, 12 September 2020, available at: https://informationrightsandwrongs.com/2020/09/12/if-ico-wont-regulate-the-law-it-must-reboot-itself/

[50] *It looks like the UK's data regulator has given up, blaming coronavirus*, Wired, 19 May 2020, available at: https://www.wired.co.uk/article/ico-data-protection-coronavirus

[51] Chris Pounder, *Draft Brexit Data Protection Regulations would undermine adequacy determination for the UK* (footnote 39, above).

Note that the amendments could have easily kept the notion of an independent Commissioner. For instance:

> 51(1). *The Commissioner is an independent public authority* responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data.

Now ask yourself a simple question: could the non-inclusion of the word "*independent*" hinder an adequacy determination on the grounds that it suggests the ICO is not "*independent*"?

The changes have been made so that the ICO continues to fall within the responsibility of the [Secretary of State of the Department of Culture Media and Sport] and does not directly report to Parliament as previous Commissioners have wanted. In addition, the Regulations remove the obligation in Article 52(4) to 52(6) [GDPR] which effectively provide for adequate resources to be allocated to the ICO, for the ICO to choose his own staff and the obligation not to starve the ICO of funding.

Will these exclusions influence any adequacy determination by the Commission? What do you think?

In our view, the UK can not be granted a positive adequacy decision unless it provides strong assurances about the independence of the ICO and about the ICO's willingness to properly enforce the law.

In the second Part of our analysis, we turn to the question of access by the UK's national security agencies to any data that may be transferred from the EU to the UK after the post-Brexit transition period, and possible onward transfers of such data to national security agencies of other third countries, including in particular the USA (which has been held by the CJEU to not provide adequate protection specifically in that regard).

- o – O – o -