"The United Kingdom is not a third country under EU law"*

*** For data protection purposes, for a certain period**

(Article FINPROV.10A CTA)

by

Douwe Korff

Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

1 January 2021

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

EXECUTIVE SUMMARY

The EU-UK Trade and Cooperation Agreement (TCA) stipulates, in Article FINPROV.10A, that, from the coming into (provisional) effect of that agreement, i.e., from 1 January 2021, for a "specified period" of four months (extendable to six months), subject to certain conditions:

> **"transmission of personal data from the Union to the United Kingdom shall not be considered as transfer to a third country under Union law"**

This means that under Article FINPROV.10A TCA, as far as transborder transfers of personal data from the EU/EEA to the UK are concerned, the UK will, for some (supposedly limited) time and subject to those conditions, be treated as if it were still an EU Member State.

*In this respect (for this period and subject to those conditions), Boris Johnson's government therefore actually did get to "*have its cake and eat it*": the UK is no longer an EU or EEA Member State, but it still gets to be treated as if it were an EU/EEA Member State.*

There are five main reasons why the stipulation in Article FINPROV.10A TCA is unacceptable in EU law:

1. the stipulation fundamentally undermines EU data protection law as guaranteed by the EU Treaties, the EU Charter of Fundamental Rights and the EU data protection instruments as interpreted by the Court of Justice of the EU;
2. as a matter of official EU policy, the issue of data protection (including in respect of transfers of personal data) should not be addressed in a free trade agreement – but Article FINPROV.10A does precisely that;
3. the conditions under which the stipulation applies are insufficient and in particular fail to address the issue of UK mass surveillance – which is a matter directly relevant to the issues of data protection adequacy and data transfers;
4. the "specified period" of four to six months can be extended by the EU and the UK at will;* and
5. the stipulation assumes that a (positive) adequacy decision on the UK will be issued within the "stipulated period", when this is far from certain (to put it mildly).

* Those who feel that since Article FINPROV.10A says it will only apply for a few months it is not a big deal should read the section in this note on the fourth point, section 3.4, in particular.

I therefore urge the European Parliament, in the process for approval of the agreement, to insist that Article FINPROV.10A be removed – or at least, that full and formal binding assurances are given that the four to six month period will not under any circumstances be further extended, not even, indeed especially not, if the Commission concludes that the UK does not provide "adequate"/"essentially equivalent" protection to personal data, given its excessive mass surveillance activities.

- o – O – o -

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

"The United Kingdom is not a third country under EU law"*

*** For data protection purposes, for a certain period**

1. The "temporary" status of the UK under the EU-UK Trade & Cooperation Agreement in relation to transfers of personal data

The EU-UK Trade and Cooperation Agreement (TCA) stipulates, in Article FINPROV.10A, that, from the coming into (provisional) effect of that agreement, i.e., from 1 January 2021, for a "specified period" of four months (extendable to six months), subject to certain conditions (discussed below, at 3.3):[1]

> **"transmission of personal data from the Union to the United Kingdom shall not be considered as transfer to a third country under Union law"**

As explained below, at 2, this is not just odd – it is nonsensical and weird. What is more, as noted at 3, the stipulation is also unacceptable. It undermines EU data protection law and is incompatible with the EU Treaties, the EU Charter of Fundamental Rights, all the EU data protection instruments (the GDPR, the Law Enforcement Directive and the Regulation on data protection in the EU institutions), and with crucial case-law of the Court of Justice of the EU. Moreover, the short "specified period" for which this clause is stipulated to apply can be extended by the EU and the UK at will – even if it becomes clear that the European Commission cannot lawfully issue a (positive) data protection adequacy decision on the UK (in particular, because of the UK's mass surveillance activities). I conclude at 4, that the European Parliament should not approve the TCA unless this dangerous clause is removed or at least strictly circumscribed.

2. Why the stipulation in the TCA is weird

The stipulation that "*transmission of personal data from the Union to the United Kingdom shall not be considered as transfer to a third country under Union law*" is strange.

The term "third country" (or "third countries") is used dozens of times in the Treaties, where it means a country that is not a member of the Union (see, e.g., Article 21(1) TEU, Article 23 TFEU). As explained by *Eurofound*, this meaning is derived from "third country" in the sense of one not party to an agreement between two other countries.[2]

But as loudly trumpeted by the Johnson Government, the UK has shaken off the "shackles" of EU membership to "regain its sovereignty" and, certainly from 1 January 2021, undoubtedly **is** a "third country" in terms of EU law".[3]

---

[1] The full text of the TCA can be found here; Article FINPROV.10A is in Part Seven, Final Provisions, on pp. 406 – 407: https://ec.europa.eu/info/sites/info/files/draft_eu-uk_trade_and_cooperation_agreement.pdf

[2] See: https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/third-country-nationals The page adds that, "*[e]ven more generally, the term is used to denote a country other than two specific countries referred to, e.g. in the context of trade relations*" and that "*[t]his ambiguity is also compounded by the fact that the term is often incorrectly interpreted to mean 'third-world country'.*"

[3] The UK formally ceased to be an EU Member State on 1 February 2020, but remained subject to many EU legal rules and procedures, including the EU data protection regimes and the jurisdiction of the CJEU, during the post-

And under Chapter V of the EU General Data Protection Regulation (GDPR), personal data may only be freely transferred: **(a)** between EU/EEA[4] Member States (Article 1(3) GDPR) and **(b)** from an EU/EEA Member State to a third country that has been held by a decision of the European Commission to provide an "adequate" level of protection of personal data (Article 45 GDPR).[5] Regular transfers of personal data from an EU Member State to a third country that does not provide "adequate" protection to such data may only take place if "appropriate safeguards" are put in place, such as Standard [Personal Data Transfer] Contract Clauses (SCCs) or approved Binding Corporate Rules (BCRs) for multinational companies (Article 46 and 47 GDPR).[6]

Those are not just some minor issues under a specific regulation. Rather, these principles are firmly underpinned by the Treaties and EU Charter of Fundamental Rights that expressly guarantee data protection as a specific, *sui generis* right. Relying on these constitutional EU instruments, the Court of Justice of the EU (CJEU) has held that "adequate protection" must be read as requiring "essentially equivalent" protection to that accorded by EU law,[7] and (as discussed at 3.1, below) that in relation to third countries that engage in excessive surveillance, further "supplementary measures" are needed to protect against such surveillance.

So what does the stipulation mean? Why is it weird? Under EU Treaty- and data protection law, there are only two kinds of cross-border transfers of personal data: transfers from one EU/EEA Member State to another EU/EEA Member State (which are free: see (a), above) and transfers from an EU/EEA Member State to a country that is not an EU/EEA Member State, a "third country" (which are only free if the third country in question has been formally held by the European Commission to provide adequate/essentially equivalent protection: see (b), above). There are no other kinds of cross-border transfers of personal data conceived of in EU data protection law (or in the Treaties).

It follows that the stipulation that "*transmission of personal data from the Union to the United Kingdom shall not be considered as transfer to a third country under Union law*" can only mean that such transmissions or transfers[8] of personal data from the EU and from the non-EU EEA countries[9] to the UK must be treated as transfers of personal data between EU/EEA Member States – that is, they will be treated as intra-EU/EEA transfers, free from all constraints under

---

Brexit "transition period". That period ended on 31 December 2020. From that moment, the UK therefore really can no longer be treated (more or less, in certain respects) as if it was still an EU Member State.

[4] The GDPR applies equally to all EU Member States and the three non-EU Member States of the European Economic Area (EEA): Iceland, Liechtenstein and Norway.

[5] Similar rules apply in relation to transfers of personal data in relation to law enforcement matters and to transfers of personal data by the EU Institutions under, respectively, the EU Law Enforcement Directive and the Regulation on processing of personal data by the EU Institutions – but in this short note I will focus on the GDPR.

[6] Under Article 49, there are also some derogations for "specific situations" but these are restrictively interpreted ad cannot be relied on for regular transfers. See the EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018, available at:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

[7] 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

[8] The terms appear to be synonymous in the TCA (indeed in the very sentence in Article FINPROV.10A) – as translations into other Union languages are likely to confirm.

[9] Subject to the agreement of those three non-EU EEA countries: see Article FINPREOV.10A(2).

Article 1(3) GDPR (rather than as transfers to a third country that are subject to the rules in Chapter V GDPR just mentioned).

In sum: Under Article FINPROV.10A TCA, as far as transborder transfers of personal data from the EU/EEA to the UK are concerned, the UK will, for some (supposedly limited) time and subject to certain conditions, , be treated as if it were still an EU Member State.

*In this respect (for this period and subject to those conditions), Boris Johnson's government therefore actually does get to "*have its cake and eat it*": the UK is no longer an EU or EEA Member State, but it still gets to be treated as if it were an EU/EEA Member State.*

In the next section, I will show why this is unacceptable in EU law.

3. Why the stipulation in the TCA is unacceptable

There are in my opinion five main reasons why the stipulation in Article FINPROV.10A TCA is unacceptable in EU law:

1. the stipulation fundamentally undermines EU data protection law as guaranteed by the EU Treaties, the EU Charter of Fundamental Rights and the EU data protection instruments as interpreted by the CJEU;
2. as a matter of official policy, the issue of data protection (including in respect of transfers of personal data) should not be addressed in a free trade agreement – but Article FINPROV.10A does precisely that;
3. the conditions under which the stipulation applies are insufficient and in particular fail to address the issue of UK mass surveillance – which is a matter directly relevant to the issues of data protection adequacy and data transfers;
4. the "specified period" of four to six months can be extended by the EU and the UK at will; and
5. the stipulation assumes that a (positive) adequacy decision on the UK will be issued within the "stipulated period", when this is far from certain (to put it mildly).

Below, I briefly discuss each of these in turn.

3.1 The stipulation fundamentally undermines EU data protection law as guaranteed by the EU Treaties, the EU Charter of Fundamental Rights and the EU data protection instruments

i. The normal regime

The GDPR regime from transfers of personal data from the EU/EEA to third countries (and the corresponding regimes in the other EU data protection instruments) are at the core of the system of protection of such data in EU law: as Article 44 GDPR and the case-law of the CJEU make emphatically clear, the regime seeks to ensure that such transfers do not "undermine" "the level of protection of natural persons guaranteed by [that] Regulation". As Recital (101) to the GDPR explains:

> Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, **when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined**, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. **In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.**
>
> (emphases added)

Following the *Schrems I* "essential equivalence" clarification, the Article 29 Working Party expanded on the requirements for an adequacy decision (the "conditions" referred to in the above quote) in its so-called "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.[10] Briefly, in line with the stipulations in Article 45(2) GDPR, adequacy assessments must comprise the following three elements:[11]

- 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.

---

[10] 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 2017/2018 referential replaced very old previous guidance in the 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

[11] For further details of the adequacy tests and information on the quite elaborate process for the adoption of an adequacy decision, see section 2 in Douwe Korff & Ian Brown, The inadequacy of UK data protection law in general, Part One (footnote 18, below).

Article 45(2)(a) GDPR adds that the last of the above assessment elements, the one related to the rule of law, 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. 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)*,"[12] in which it set out important initial standards in that regard.

In July 2020, the CJEU issued its *Schrems II* judgment,[13] in which it assessed the surveillance regime of the USA with reference to EU fundamental rights standards, and found it wanting. In particular, access by the US national security agencies to personal data that are transferred to the USA is not limited to what is necessary and proportionate in relation to national security: US law allows for indiscriminate access to such data by those agencies, and provides no effective independent remedies to EU individuals who may be affected by those excessive US agencies' powers.[14] In two even more recent judgments, *Privacy International (PI)*[15] and *La Quadrature du Net (LQDN)*,[16] the Court provided further clarification on the fundamental EU legal requirements relating to mass surveillance.

Following these judgments, the European Data Protection Board, in November 2020, produced a recommendation containing a set of **updated** "**European Essential Guarantees for surveillance measures**" (hereafter: **EEGs**).[17]

In a two-part submission to the EU institutions involved in the taking of a possible adequacy decision on the UK, Prof. Ian Brown and I concluded that UK data protection as applied after the

---

[12] 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

[13] CJEU Grand Chamber judgment in case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("*Schrems II*"), 16 July 2020, available at: http://curia.europa.eu/juris/liste.jsf?num=C-311/18

[14] See the Court's conclusions in paras. 184 – 185 and 197 of the judgment.

[15] CJEU Grand Chamber judgment in Case C-623/17, *Privacy International*, 6 October 2020, available at: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9CC0631635C4B49686319F07615E3E75?text=&docid=232083&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=10014575

[16] CJEU Grand Chamber judgment in Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, 6 October 2020, available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=10014575

[17] EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf
The recommendations build on the earlier EEGs (WP237, footnote 11, above), but takes into account the important subsequent case-law of both the Luxembourg and Strasbourg Courts, in particular *Schrems II*.

post-Brexit transition period, in particular the so-called "UK GDPR" that is similar to but not quite the same as the EU GDPR, did not meet the criteria set out in the EU Adequacy Referential and, more specifically, that the UK, in intimate cooperation with the USA, is engaged in mass surveillance over international communications data under rules that manifestly fail to meet the European Essential Guarantees – and that the UK should therefore not be granted a (positive) adequacy decision.[18]

ii. The "temporary" regime created by Article FINPROV.10A TCA

The point to be made here is that under the GDPR (and the other EU data protection instruments), unimpeded transfers of personal data to any third country are only allowed if the third country in question is held by the Commission, in an elaborate process, to provide adequate/essentially equivalent protection to such data.

Article FINPROV.10A TCA drives a horse and cart through this by pretending that (for the specified period and subject to the specified conditions) transfers of personal data to the UK are not "transfers to a third country". It does so without any actual assessment of the UK data protection regime as it will apply from 1 January 2021, and without following the process for adequacy decisions. Rather, as it is put in a "Declaration on the Adoption of Adequacy Decisions with respect to the United Kingdom" adopted together with the Trade and Cooperation Agreement:[19]

> The Parties [i.e., the EU and the UK] take note of **the European Commission's intention to promptly launch the procedure for the adoption of adequacy decisions with respect to the UK under the General Data Protection Regulation and the Law Enforcement Directive**, and its intention to work closely to that end with the other bodies and institutions involved in the relevant decision-making procedure.
>
> (emphases added)

In other words, pending the issuing of an actual adequacy decision (or a decision not to issue one) on the UK, the UK is effectively granted the benefits of a positive adequacy decision without one having been issued (or even, it would seem, prepared) and without the process for such a decision being followed.

In fact, the situation is worse than that: as noted earlier, for the purpose of personal data transfers from the EU/EEA, Article FINPROV.10A effectively grants the UK "temporarily" the status of an EU Member State.

---

[18] Douwe Korff & Ian Brown, The inadequacy of UK data protection, submission to the EU bodies involved in assessing whether the UK should be granted a positive adequacy decision after the post-Brexit transition period, 9 October 2020, Part One (general adequacy), available at:
https://www.ianbrown.tech/2020/10/09/the-uks-inadequate-data-protection-framework/
Idem, Part Two, (*re* UK surveillance), 30 November 2020, available at:
https://www.ianbrown.tech/2020/11/30/the-uks-intelligence-activities-and-gdpr-inadequacy/
See also the Executive Summary of that submission that contains a discussion of the implications of the findings, available at:
https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-ExecSumm-DK-IB201130.pdf

[19] Included in a list of declarations issued with the TCA, on p. 25, available at:
https://ec.europa.eu/info/sites/info/files/draft_eu-uk_declarations.pdf

This is fundamentally incompatible with the GDPR and the case-law of the CJEU, rooted deeply in the Treaties and the Charter. There is simply no legal basis for the creation of the legal fiction of a third country that is "treated" for some purpose – here, for the purpose of personal data transfers – as not being a third country, but rather as if it were (still) an EU Member State.

The declaration also suggests that the issuing of a positive adequacy decision is just a matter of time – when that should be far from a forgone conclusion, as noted at 3.5, below.

3.2 The issue of data protection (including in respect of transfers of personal data) should not be addressed in a free trade agreement

"*The protection of personal data is non-negotiable in [EU] trade agreements*"[20]

The European Parliament and the European Data Protection Supervisor rightly take the view that data protection rules cannot be included in EU – third country trade agreements.[21]

On 31 January 2018, the European Commission adopted a set of "horizontal provisions for cross-border data flows and for personal data protection (in EU trade and investment agreements)", without releasing the text – but shortly after, the provisions were leaked.[22] They stipulated that Investor-State Dispute Settlement (ISDS) schemes, and more in particular the then proposed Investment Court System "do[ ] not apply" to the rules on cross-border data flows, or on protection of personal data and privacy (Article B.2 and 4). They added, for the avoidance of all doubt ("For greater certainty"), that the rules on cooperation on regulatory issues with regard to digital trade – which committed the parties to a "dialogue [and cooperation] on regulatory issues raised by digital trade" – also "shall not apply to a Party's rules and safeguards for the protection of personal data and privacy, including on cross-border data transfers of personal data" (Article X.3).

In simple terms: the EU legally cannot "barter" data protection in trade negotiations, either in substance or in terms of formalities (ISDS schemes). On the contrary, in the context of trade agreements and trade data flows, the continued full protection of personal data that are subject to EU data protection rules (in particular, in such contexts, to the GDPR) must be ensured. The data transfer rules in the GDPR (and the other EU data protection instruments) cannot simply be set aside or overruled in a trade agreement – such as the EU-UK Trade and Cooperation Agreement.

But that is of course precisely what the insidious Article FINPROV.10A does.

---

[20] European Parliament resolution of 12 December 2017 "*Towards a digital trade strategy*" (2017/2065(INI)), Section V, available at: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_EN.pdf

[21] Cf. European Parliament, Report containing the European Parliament's recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI)), 25 January 2016, p. 10, para. 1(c)(iii), available at: https://www.europarl.europa.eu/doceo/document/A-8-2016-0009_EN.html
Giovanni Buttarelli, former European Data Protection Supervisor, *Less is sometimes more*, blog, 18 December, 2017, with reference to the Commission President Juncker's 2016 State of the Union address to the European Parliament, available at: https://edps.europa.eu/press-publications/press-news/blog/less-sometimes-more_en
https://ec.europa.eu/commission/priorities/state-union-speeches/state-union-2016_en

[22] They are available here:
https://www.politico.eu/wp-content/uploads/2018/02/Data-flow-provisions-POLITICO.pdf

3.3 The conditions under which the stipulation applies are insufficient and in particular fail to address the issue of UK mass surveillance – which is a matter directly relevant to the issue of data protection adequacy

The stipulation in Article FINPROV.10A(1) that the treatment of transfers of personal data from the EU[23] to the UK must be treated as "not a transfer to a third country" – i.e., as, in effect, as an EU/EEA-internal transfer – is conditional; this benefit only applies:

> provided that the data protection legislation of the United Kingdom on 31 December 2020, as it is saved and incorporated into United Kingdom law by the European Union (Withdrawal) Act 2018 and as modified by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 201987 ("the applicable data protection regime"), applies and provided that the United Kingdom does not exercise the designated powers without the agreement of the Union within the Partnership Council.
>
> (emphases added)

The "designated powers" are listed in Article FINPROV.10A(3) and discussed below, at ii.

The "applicable data protection regime" referred to consists mainly of the so-called "UK GDPR",[24] a UK law that initially fairly closely follows the EU GDPR (but not fully: see below, at i), but that can be changed (under the UK European Withdrawal Act) by ministerial order in almost all respects. This latter issue is what the second proviso refers to: the odd treatment of the UK for data transfer purposes as if it were not a third country only applies for as long as the UK does not exercise certain of the relevant powers to change the rules; if it wants to exercise those powers during the "stipulated period" (discussed below, at 3.4), it needs the agreement of the Partnership Council established to supervise the implementation of the TCA, i.e., in effect, of the EU.

This raises **three questions**. First of all: whether "the applicable [UK] data protection regime" as it will be on 1 January 2021, i.e., mainly the UK GDPR, is "adequate"/"essentially equivalent" to the EU regime. Secondly: whether the second proviso (relating to changes made to the UK regime) covers all relevant matters. And third: how this relates to the UK mass surveillance activities.

All of these issues are addressed in the two-part submission Ian Brown and I made recently,[25] so below brief summaries from our conclusions are used.

i. Whether the UK GDPR as it will be on 1 January 2021 is "adequate"/"essentially equivalent" to the EU GDPR

In Part One of our submission we noted the following:[26]

---

[23] And from the non-EU EEA countries: see footnote 9, above.

[24] On the issue of whether Article FINPROV.10A also applies to the British territories of Guernsey, Jersey and the Isle of Man, and to Gibraltar, see footnotes 27 and 28, below.

[25] See footnote 18, above.

[26] As summarised in the Executive Summary of our submission. For the link, see again footnote 18, above. The full discussions of the issues summarised here (and in the next sub-section) can be found in Part One of our submission (with references).

Deficiencies in the "core" substantive requirements of the UK's post-Brexit data protection regime:

- Under the UK Digital Economy Act 2017, personal data are more narrowly defined than in the EU GDPR; consequently, they can be much more widely shared and used than would be allowed under the EU GDPR. 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).
- Although held to be lawful by the UK courts, the so-called "immigration exemption" in the UK data protection legislation (that directly affects all EU citizens resident in the UK) is excessive in terms of the EU GDPR.
- In both these respects, UK data protection already is clearly not "essentially equivalent" to the EU GDPR.

Deficiencies in the "procedural/enforcement" guarantees in the UK's post-Brexit data protection regime:

- 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. Moreover, there are major, long-standing questions about its independence, which are reinforced by differences between the EU GDPR and the "UK GDPR".

In view of the above, it is in my opinion (and in the opinion of my colleague Ian Brown, and others) highly doubtful whether "the applicable [UK] data protection regime" as it will be on 1 January 2021, i.e., mainly the UK GDPR, is "adequate"/"essentially equivalent" to the EU regime.

ii. Whether the proviso relating to changes made to the UK regime covers all relevant matters

Ian Brown and I noted a further major deficiency in the UK regime, the issue of "onward transfers", as follows:

The issue of "onward transfers":

- The "UK GDPR" 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 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. 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 (and in relation to the sharing of intelligence data, as noted at iii, below).

- These matters 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) to include the free flow of data (including personal data) in such agreements. This is in direct contrast to the EU policy under which personal data may not be included in FTAs (see section 3.2, above). 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 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 that the USA does not ensure adequate/essentially equivalent protection because of its surveillance regime.
- **Both the above matters, and their combination, will lead to the UK effectively becoming a "data laundering haven" if it were to be granted a positive adequacy decision – *or, I may add here, if it were to conclude such an FTA with the USA during the "specified period".***

Article FINPROV.10A lists, in its third paragraph, a number of "designated powers" that the UK must not use during the "specified period". These all relate to transfers of personal data from the UK to other countries (other than EU/EEA countries) on the basis of UK adequacy decisions, UK- (but not EU-) approved standard contract clauses (SCCs), Binding Corporate Rules (BCRs), codes of conduct, certification schemes or "administrative arrangements" between public authorities. **In other words, for the time being (during the "specified period"), the UK may not facilitate transfers of personal data on these bases.**[27]

However, the "designated powers" do not appear to cover – i.e., during the "specified period" the TCA does not stand in the ways of – transfers authorised on the basis of overriding public interests (Section 18 of the UK GDPR). Article FINPROV.10A also does not address the possibility that the UK will include free personal data flows in UK – other countries trade agreements.

Moreover, Article FINPROV.10A only bars the UK from exercising these powers "[f]or the duration of the specified period" – which means from 1 January 2021 until the end of this period (as discussed below, at 3.4). This suggests that the UK declaration that Gibraltar provides "adequate" protection to personal data issued before that period started, noted above, is not covered – and that therefore personal data transferred during the specified period from the EU/EEA to the UK may be further, freely, "onwardly" transferred to that territory even though it has not been held to provide "adequate"/"essentially equivalent" protection in terms of the EU GDPR.[28]

---

[27] Article FINPROV.1 (on the territorial scope of the whole TCA) stipulates, in its second paragraph, that:

> This Agreement also applies to the Bailiwick of Guernsey, the Bailiwick of Jersey and the Isle of Man to the extent set out in Heading Five [Fisheries] and Article OTH.9 [Geographical application] of Heading Six [Other provisions] of Part Two of this Agreement.

The EU has issued adequacy decisions on these territories that (for now) remain in effect (but see the comments by Ian Brown and me in section 4.2 of the Executive Summary of our submission). Presumably, therefore, during the "specified period" personal data transferred from the EU/EEA to the UK may be freely onwardly transferred to these territories.

[28] However, against this is a stipulation in the third paragraph of Article FINPROV.1 (see previous footnote), that "This Agreement shall neither apply to Gibraltar nor have any effects in that territory." It follows that Article FINPROV.10A also "does not apply to Gibraltar". The legal situation in relation to onward transfers of personal data from the UK to Gibraltar is therefore unclear.

Other issues not covered:

The "designated powers" actually fail to include the even more concerning powers of the UK, from 1 January 2021, to divert from the EU GDPR, under the European Union (Withdrawal) Act, and to limit national and international judicial control. As summarised by Brown and me:

- The UK Government has made clear that it wants to diverge from the EU standards, including from the EU data protection standards, in the near future. Moreover, although the "UK GDPR" that will apply from 1 January 2020 will, on that date, still be quite close (although not quite the same) as the EU GDPR, the UK's European Union (Withdrawal) Act expressly allow a "coach and horse" to be driven through the UK regulation: essentially all its provisions can be changes by ministerial decree.
- 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, starting with the interpretations of the Convention by the European Court of Human Rights. The latter would be in line with the UK Government's express willingness to take action against what it perceives as judicial "overreach" domestically.

In other words: Article FINPROV.10A does not appear to prevent the UK government changing the UK GDPR (using the powers it has to do so under the European Union (Withdrawal) Act), even during the "specified period", to further divert from the EU GDPR and to become even less "adequate", to provide even more clearly less than "essentially equivalent" protection, than is provided for under the EU GDPR. It also does not appear to prevent the UK government from withdrawing, in whole or in part, from the ECHR or from following the interpretations of the Convention by the Strasbourg Court (and of course the UK is also no longer subject to the jurisdiction of the CJEU).

Changes to the UK data protection regime with the agreement of the EU

There are two related but distinct issues to be mentioned in this section. The first is that changes made to "the applicable data protection regime" (i.e., in particular, the UK GDPR), under the "designated powers" or otherwise, in order to align that UK regime with the EU regime does not invalidate the application of Article FINPROV.10A (see paras. 6 and 7(b) of that article). This includes the UK declaring another third country to provide "adequate" protection in terms of the UK GDPR if that third country is held by the European Commission to provide "adequate"/ "essentially equivalent" protection in terms of the EU GDPR. This is not controversial since it is unlikely to undermine the protection accorded by EU data protection law.

However, Article FINPROV.10A(7)(a) also provides that "*[amendments to the UK regime] made with the agreement of the [European] Union within the Partnership Council*" shall also not be regarded as amendments to the UK regime that would invalidate the application of the main stipulation (that transfers of personal data from the EU/EEA to the UK shall not be regarded as transfers of personal data to a third country).

This is much more problematic. It would appear to allow the political organs of the EU (as represented in this Partnership Council) to allow the UK to amend its (in my opinion, already deficient) data protection regime in ways that would further depart from the EU adequacy and "European Essential Guarantees" standards. And this can apparently be done without reference to the bodies that are to be involved in adequacy decisions under the normal regime (see section 3.1.i, above).

This allows for a totally unacceptable by-passing of the EU legal system for personal data transfers to third countries, in relation to transfers to the UK.

iii. How the provisos relate to the UK mass surveillance activities

In three words: **they do not**. **Not at all**. While under GDPR adequacy standards, as emphatically endorsed and further strengthened by the CJEU, access to personal data transferred to a third country from the EU/EEA by agencies of that third country is a major issue, especially in relation to third countries that indulge in undue mass surveillance, **the issue is simply ignored by Article FINPROV.10A TCA**.

In this respect, Ian Brown and I concluded as follows:[29]

As to the UK surveillance practices:

- The UK, working jointly with the US National Security Agency (NSA), taps into a large number of selected Internet communications link (especially but not only underseas cables), including cables through which most of the communications of EU individuals, institutions and officials travel (in particular, most EU – UK – USA communications). These communications include not only emails and social media exchanges but also the data flows between EU users of US-based cloud services and the relevant US cloud servers.
- Very large amounts of data – including all communications metadata (including traffic- and location data) are extracted by the UK from all selected bearers indiscriminately, in bulk, and retained for some time.
- The metadata are highly revealing of the lives of potentially hundreds of thousands of individuals to which they may relate, but the vast majority of data subjects to which the metadata relate – which for many selected bearers will include large numbers of EU persons – will have no links with terrorism, threats to national security or serious crime.
- While much of the other data are filtered out fairly quickly through "simple" or "complex" queries, the metadata and the not-filtered-out data are retained for longer, to allow for their use in algorithmic analyses and profiling.
- At least some of those data are retained for purposes that are not aimed at countering serious threats to national security, but rather, to gain some politically or economically advantageous insights into actions of adversaries and allies alike.
- The not-filtered-out data, including all metadata, are subject to automatic analyses by means of self-learning (AI-based) algorithmic datamining, to "identify" (i.e., label) individuals as or linked to "Subjects of Interest" ("SoI") – but this processing suffers from major, unavoidable defects: built-

[29] As summarised in the Executive Summary of our submission. For the link, see footnote 17, above. The full discussions of the issues summarised here can be found in Part Two of our submission (with references).

in biases, mathematically unavoidable excessive numbers of "false positives" or "false negatives" (or both), and the fact that because of their complexity they become effectively unchallengeable. It is unavoidable that many individuals who are labelled or linked to "SoI" are innocent and have no links to serious crime or terrorism.

As to the law:

- Under UK data protection law, metadata are not meaningfully protected against undue access and bulk collection by the UK intelligence agencies.
- The UK Investigatory Powers Act clearly does not "itself define" the scope and limitations of the use of the powers it grants the intelligence agencies, in particular in relation to direct access to the systems of communication and Internet service providers, or to direct tapping into underseas cables. The IPA therefore does not meet the requirement set in that regard by the CJEU in *Schrems II*.
- The UK IPA rules that allow for the extraction, in bulk, of at least all the metadata of all communications that flow through a selected bearer, are clearly incompatible with the standards set out in a range of CJEU judgments and arguably (given the now-recognised inherent sensitivity of metadata) compromise the very essence of the rights to privacy, confidentiality of communications and data protection.
- The law allows for broadly phrased bulk interception warrants and for vague search criteria to be applied to stored data; the law itself does little to preclude targeting of improper targets. Rather, almost complete reliance is placed on the institutional oversight of the use of the powers. This too is at odds with the EU requirements.
- Rather than oversight over "the selection of bearers, the application of simple selectors and initial search criteria, and the complex searches which determine which communications are read" being clearly and expressly provided for in the law (i.e., in the IPA), the issue has been left to an "assurance" from the Home Office to the Independent Reviewer of Terrorism Legislation that such oversight is "inherent" in various clauses in the Act. That is hardly a hard-and-fast legal assurance; the assurance was not even made by a minister in Parliament.

  The situation in relation to oversight over complex selectors and search criteria is still unclear, while oversight over the much more sophisticated data mining analyses appears to not have been addressed at all. This means the situation in this regard, too, clearly does not (yet) meet the EU standards as set out, in particular, in the CJEU *LQDN* judgment, referenced in this regard in the EEGs.
- The remedies accorded by the Investigatory Powers Tribunal were essentially held to be effective in terms of the ECHR, partly because the Tribunal was clearly independent and impartial, and issued strong rulings in appropriate cases – but also because in its rulings it had the power and the duty to ensure that both practice and the law were compliant with EU law including the Charter of Fundamental Rights.

  But of course, this will fundamentally change from 1 January 2021, when the IPT will no longer be able to rely on EU law (including the Charter) in assessing the validity of various elements of the UK surveillance regime – which is deficient in several respects as shown above.

  This raises serious doubts as to whether, at least in relation to the compatibility of the legal regime as such with European fundamental rights standards, the IPT will still be able to provide a judicial remedy in terms of Article 6 ECHR, or even an "effective remedy" in terms of Article 13 ECHR, or

an "effective remedy before a tribunal" in terms of Article 47 of the Charter (to which much attention was given by the CJEU in its *Schrems II* judgment).

- Data on individuals in the EU, extracted in bulk from the underseas cables by GCHQ, and the results of the analyses of those data, are shared with the USA – which has been specifically held to not provide "adequate"/"essentially equivalent" protection to personal data in *Schrems II*.
- The carrying out of automated profiling by GCHQ (in cooperation with the US NSA), and the taking of decisions about individuals – including EU individuals – on the basis of the (secret) results of that profiling, does not meet the requirements of Article 22 GDPR – and this deficiency in UK law and practice, too, stands in the way of a positive adequacy decision on the UK.

Overall conclusion reached in relation to surveillance:

- In our opinion, it is highly doubtful whether the processing of personal data by UK intelligence agencies, especially its bulk collection of communication data, is in line with the EU Charter of Fundamental Rights. In particular, its indiscriminate bulk collection of communications metadata ("related communications data") from selected "bearers" in the underseas communication cables would appear to be contrary to principles established by the European Court of Human Rights (*Big Brother Watch v. the UK*) and the CJEU (*Tele2/Watson*, *Digital Rights*, *Schrems II*, *Privacy International* and *La Quadrature du Net*), as reflected in the recent EDPB's "European Essential Guarantees for Surveillance Measures".

In our opinion, on the basis of the conclusions reached in Parts One and Two, summarised above, the UK can therefore not be granted a positive adequacy decision under Article 45 GDPR.

Here, I note that: Article FINPROV.10A does not in any way affect – let alone limit – the mass surveillance activities of the UK intelligence agencies (carried out hand-in-glove with the USA's National Security Agency). This flies in the face of the CJEU's *Schrems II* judgment in particular, in which the Court ruled that the NSA's practices and the limited remedies against them available to EU persons meant that the USA should not be held to provide "adequate"/"essentially equivalent" protection to personal data.

Note: The fact that during the "specified period" the UK is effectively treated as an EU Member State for the purpose of personal data transfers is relevant here: as noted (and criticised) by Brown and me in our submission,[30] under the EU Treaties the EU has no competence in relation to national security activities of the EU Member States – but it does have the power to take the national security activities of third countries into account in determining whether the latter's laws and practices provide "adequate"/"essentially equivalent" protection to personal data. Whether the exclusion of any assessment of the UK surveillance activities was specifically intended by declaring that transfers of personal data to that country to not constitute transfers to a third country, I do not know. But it is very notable that the Trade and Cooperation Agreement totally ignores the issue.

[30] See in particular the Executive Summary, section 4.4.

3.4 The "specified period" of four to six months can be extended by the EU and the UK at will

As noted earlier, Article FINPROV.10A(1) stipulates that that article only applies "[f]or the duration of the specified period", and that period is specified in the fourth paragraph as follows:

> The "specified period" begins on the date of entry into force of this Agreement [i.e., 1 January 2021] and, subject to paragraph 5, ends:
>
> (a) on the date on which adequacy decisions in relation to the UK are adopted by the European Commission under Article 36(3) of Directive (EU) 2016/680 and under Article 45(3) of Regulation (EU) 2016/679, or
>
> (b) on the date four months after the specified period begins, which period shall be extended by two further months unless one of the Parties objects;
>
> whichever is earlier.

(Paragraph 5 adds that the "specified period" – and with it the special status of the UK in relation to data transfers – also ends if "during the specified period, the United Kingdom amends the applicable data protection regime or exercises the designated powers without the agreement of the Union within the Partnership Council.)

In early online comments, several commentators have shrugged off the importance of Article FINPROV.10A on the basis that it only applies for a maximum of six months, and will cease to apply on 1 July 2021 latest. As they noted, this certainly does not leave time for an adequate legal challenge.

However, in this they fail to note one major issue – which is that Article INST.1 of the TCA, on the Partnership Council that "*shall oversee the attainment of the objectives of this Agreement [the TCA] and any supplementing agreement*", stipulates in its fourth paragraph, at (c), that:

> **The Partnership Council shall have the power to … adopt, by decision, amendments to this Agreement** or to any supplementing agreement in the cases provided for in this Agreement or in any supplementing agreement
>
> (emphasis added)

The Partnership Council has two co-chairs, one representing the EU and one the UK (Annex Inst, Rule1(1) – which does not mention any other members). They take their decisions "by mutual consent" (Rule 1(2)).[31] Each party "***may*** decide on the publication of the decisions and recommendations of the Partnership Council in its respective official journal or online" (Rule 10(2), emphasis added). In other words, they may also take decisions without publishing them. Moreover:

> If the Union or the United Kingdom submits information that is confidential or protected from disclosure under its laws and regulations to the Partnership Council, the other party shall treat that information received as confidential.
>
> (Rule 10(3))

[31] They may also delegate the power to take the decision mentioned in Article INST.1 (like most other decisions) to the Trade Partnership Committee or one of the Specialised Committees, established by Article INST.2 (Article INST.1(4)(f)).

In other words, **anything in the Trade and Cooperation Agreement, *including the "specified period" for the application of Article FINPROV.10A*, can be amended by agreement between the parties, i.e., by agreement between the EU and the UK.** And any such decision may take place on the basis of secret information (if either the EU or the UK demands that) – and can even be kept unpublished.

It is perhaps unlikely that any decision to extend the "specified period" during which the UK is treated, in relation to transborder flows of personal data, as if it were still an EU Member State would be kept secret; such a decision would need to be made public in order for companies and public authorities to rely on it. But it is not that unlikely that the UK would present the EU with "confidential" information to persuade the latter to extend the period, for instance on the basis that not to do so would harm UK and EU national security.

And of course, the process for decision-making in the Partnership Council falls far short of the process for the adoption of an adequacy decision under the GDPR. The EDPB would not have to give an opinion on any such proposed decision, and neither the UK nor the European Parliament would have to be consulted.

For the next few months, but possibly for much, much longer, the TCA effectively by-passes the GDPR process altogether – with an outcome that puts the UK in an actually better position than other countries considered for adequacy, in that the UK's surveillance activities, unlike those of other third countries including the USA, are left conveniently out of consideration.

In my opinion, if Article FINPROV.10A is weird and unacceptable even in the short term, any extension of the "specified period" set out in it by the Partnership Council would be scandalous and an affront to the rule of law, the Treaties and the Charter.

3.5 It is wrongly assumed that the UK will shortly be granted a positive adequacy decision

The numbering of Article FINPROV.10A suggests that it was inserted between Articles FINPROV 10 and 11 at a late stage. Presumably, earlier on it was thought that EU adequacy decisions on the UK (one under the GDPR and one under the Law Enforcement Directive) could and would be issued before the end of (and with effect immediately from the end of) the post-Brexit transition period: in that case, there would have been no need for the article.

The drafters of Article FINPROV.10A and of the Declaration on the Adoption of Adequacy Decisions with respect to the United Kingdom also presumably assumed that such a decision could and would be issued within the "specified period" of four to six months. In contrast, Ian Brown and I strongly believe that the UK can not and should not be granted a positive adequacy decision unless: [32]

- The definition of "personal data" in the UK Digital Economy Act is brought into line with the definition of that term in the (EU) GDPR;
- The application of the immigration exemption in the UK Data Protection Act 2018 (and its successor in the "UK GDPR") is significantly tightened, made clear and foreseeable in its

[32] Again as summarised in the Executive Summary of our submission, at 3. For the link, see footnote 18, above.

application, and is limited to what is objectively necessary and proportionate in a democratic society;

- The UK provides binding assurances that it will not significantly diverge from the EU data protection standards, but rather, will maintain a data protection regime that is and will at all times be "essentially equivalent" to the EU regime; and more specifically, that it will not use the enabling provisions in the UK European Union (Withdrawal) Act to create such divergence;
- The UK agrees to not include free personal data flows in Free Trade Agreement (FTAs) with third countries that have not been held by the EU to provide adequate/essentially equivalent protection to personal data compared to the EU, including in particular the USA;
- The UK agrees to remain a full and faithful party to the European Convention on Human Rights and will continue to allow its courts to apply UK law in accordance with the Convention and European Court of Human Rights case-law, under the UK Human Rights Act;
- The UK provides strong assurances about the independence of the ICO and about the ICO's willingness to properly enforce the law; and
- **The UK fundamentally revises its surveillance law and practices to bring them into line with the European Essential Guarantees**, including by:

✓ providing meaningful protection to metadata;

✓ ending indiscriminate bulk extraction of communications data from selected Internet "bearers";

✓ setting out the limitations of surveillance in the law itself;

✓ providing explicitly, in the law, for full oversight over "the selection of bearers, the application of simple selectors and initial search criteria, and the complex searches which determine which communications are read";

✓ explicitly ensuring that the Investigatory Powers Tribunal can fully apply the ECHR through the Human Rights Act;

✓ bringing the profiling it carries out for intelligence purposes in line with the EU rules; and

✓ amending its intelligence data sharing agreement (i.e., the UKUSA Agreement) to limit the intelligence data sharing in a way that is compatible with European fundamental rights law.

The UK may be unwilling to make these changes. It is keen to develop a "data-driven economy" in which data, including personal data, can be very freely shared and used – more readily than allowed under the EU GDPR. It wants to keep the closest of tabs on "foreigners" to control immigration. And it is deeply dedicated to the US and "5EYES" intelligence arrangements under which it carries out its mass surveillance (also of European people and institutions). But as Ian Brown and I concluded in our submission:

> The UK will have to choose: it either brings its law and practices in line with the European minimum standards by accepting the conditions outlined above, and can then enjoy free data exchanges with the EU; or it will have to face and accept the negative consequences of not providing "essentially equivalent" protection to personal data as are guaranteed in the EU.

The EU – UK Trade and Cooperation Agreement should not be used by the parties to that agreement in such a way as to relieve the UK of that choice.

4. Conclusion

Article FINPROV.10A fundamentally undermines EU data protection law as guaranteed by the EU Treaties, the EU Charter of Fundamental Rights and the EU data protection instruments as interpreted by the CJEU. It drives a horse and cart through the delicate regimes on transfers of personal data, established by the GDPR, the Law Enforcement Directive and Regulation 2018/1725.

The (apparently late) inclusion of the article in the EU – UK TCA demonstrates why data protection should be left out of such instruments. The conditions for the special treatment of the UK fail to address existing deficiencies in the UK data protection regime and, especially, ignore the mass surveillance carried out by the UK, under legal rules that manifestly fail to meet the conditions set by the Court of Justice of the EU in *Schrems II* and in the EDPB's "European Essential Safeguards" for surveillance.

These are matters of principle: Article FINPROV.10A should therefore never have been included in the EU – UK CTA.

If it is not removed from the agreement, it should at the very least[33] end as suggested in its terms, no later than six months from today (1 January 2021).

I therefore urge the European Parliament, in the process for approval of the agreement, to insist that Article FINPROV.10A be removed – or at least, that full and formal binding assurances are given that the four to six month period will not under any circumstances be further extended, not even, indeed especially not, if the Commission concludes that the UK does not provide "adequate"/"essentially equivalent" protection to personal data, given its excessive mass surveillance activities.

- o – O – o -

Douwe Korff (Prof.)
Cambridge, 1 January 2021

[33] I am generally reluctant to include a "softer" option in important recommendations, since too often those to whom they are addressed (if they take note of them at all) will quickly go for the easiest solution. However, in this case it may be unrealistic to expect the EU Council and Commission and the UK Government to agree to remove Article FINPROV.10A from the TCA. In that case, it becomes absolutely essential to ensure that the "specified period" provided for in the article is not extended (by the use of Article INST.1(4)(c).