Douwe Korff & Ian Brown

The inadequacy of UK data protection law in general and in view of UK surveillance laws

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

EXECUTIVE SUMMARY & DISCUSSION OF THE IMPLICATIONS

Executive Summary 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

30 November 2020

Douwe Korff & Ian Brown

The inadequacy of UK data protection law – Executive Summary

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, comparative report covering Colombia, DR Congo, Egypt, France, Germany, India, Kenya, Myanmar, Pakistan, Russia, South Africa, Turkey, UK, 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.

Acknowledgments:

The authors are grateful to **Eric King** and **Jim Killock** for reviewing their summaries of the UK legal regimes relating to mass surveillance and bulk data collection.

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

All errors of course remain solely ours.

CONTENTS OF THE EXECUTIVE SUMMARY:

- o – O – o -

1. Summary of conclusions reached in Part One

Deficiencies in the "core" substantive requirements of the UK's post-Brexit data protection regime:[1]

- Under the UK Digital Economy Act 2017, personal data 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.
- 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.

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".

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

[1] **Stop press:** Chris Pounder has since we wrote Part One of our submission provided a useful further overview of the issues on which the UK data protection regime will differ (and to some extent already differs) from the EU GDPR. This is available at: https://amberhawk.typepad.com/files/blog19nov2020.pdf

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 (see below, at 4.2). 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 (see again below, at 4.2). 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 2, 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. 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.**

2. Summary of conclusions reached in Part Two

In Part Two, we reached the following conclusions with regard to the UK surveillance practices and laws:

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-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.

3. Conditions that should be met before the UK can be granted a positive adequacy decision

In our opinion, it follows from the above that the UK should not be granted a positive adequacy decision <u>unless</u>:

- 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 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 provided strong assurances about the independence of the ICO and about the ICO's willingness to properly enforce the law;
- **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 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.

4. Implications

NB: The main purpose of our submission was to assess the compatibility of UK surveillance with EU law and the European Essential Guarantees for surveillance, and to draw conclusions as to whether, in our opinion, the European Commission should, or should not, issue a positive adequacy decision on the UK under Article 45 GDPR, or under what conditions. We have done that in Parts One and Two of the submission.

However, we feel that it would be useful for us to also add some comments on the implications, for the UK and others (including the EU Member States) if the Commission were to agree with us and not issue such a decision. We do this below. These comments are not intended to be in any way conclusive. Rather, we wish to alert the recipients of this submission to these issues, to encourage informed debate on them.

4.1 Implications for the UK

The obvious implication of a decision by the Commission not to issue a positive adequacy decision on the UK would be that the UK would have to be treated like any other third country that had not been granted a positive adequacy decision. This would mean that regular transfers of personal data that are processed subject to the EU GDPR (or, for the EU Institutions, Regulation 2018/1725)[2] to the UK would be permitted only if "appropriate safeguards" were put in place between the EU-based data exporter and the UK-based data importer.

Those include, for regular data transfers within a group of enterprises, approved Binding Corporate Rules (BCRs); for other companies, standard contract clauses (SCCs); for the EU institutions, data transfer agreements specifically approved by the European Data Protection Supervisor; and for public bodies in the EU in relation to processing subject to the GDPR, "administrative arrangements" that have been authorised by the relevant data protection authority (see Article 46 GDPR).

However, these do not suffice in relation to third countries that engage in undue surveillance (surveillance that does not meet the European Essential Guarantees for surveillance issued recently by the European Data Protection Board). Rather, as the Court of Justice of the EU has made clear in its *Schrems II* judgment, in relation to such third countries, "supplementary measures" must be adopted to ensure that the transferred data will be protected against the undue surveillance. The EDPB has also recently issued initial guidance on what this may entail. If there are not "supplementary measures" that can effectively protect against undue surveillance in the third country concerned, the data may not be transferred.

Suffice it to note here that given the sweeping surveillance carried out by the UK's GCHQ, and its intimate cooperation with the USA's NSA, these EU requirements will create very significant obstacles to transfers of personal data from the EU to the UK.

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, at 3, 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.

[2] EU adequacy decisions adopted under the GDPR also apply to transfers under that regulation.

4.2 Implications for the other "British Islands" and Gibraltar

Guernsey, the Isle of Man and Jersey were all granted positive adequacy decisions by the EU in, respectively, 2003, 2004 and 2008 – essentially on the back of the fact that the UK was an EU Member State, and that their data protection laws closely followed UK data protection law. Those laws will continue to be brought into line with UK law, i.e., in the near future, with the "UK GDPR".

There can be no doubt that the UK will declare all these territories as providing "adequate" protection of personal data in terms of the "UK GDPR" after the end of the post-Brexit transition period – thereby allowing free transfers of personal data from the UK to these territories, including any data that may first have been transferred to the UK from the EU.

And this will undoubtedly be reciprocal: the UK will be held to provide "adequate" protection in terms of the territories' post-transition laws – thereby allowing free transfers of personal data from these territories to the UK, including any data that may first have been transferred to the territories from the EU.

Moreover, at the time of these adequacy decisions – all issued prior to the 2013 Snowden revelations – the question of surveillance was not considered. However, it should be noted that the surveillance powers of the UK intelligence agencies including GCHQ all apply equally to these other "British Islands" (as they are referred to in UK law).

In our opinion, it must follow that the (currently still in force) adequacy decisions on Guernsey, the Isle of Man and Jersey cannot be maintained after the end of the post-Brexit transition period. If they are not revoked or suspended, they would become "data laundering havens" (just as the UK would become if it were to be granted an adequacy decision in spite of our findings: see above, at 1 (last indent)).

This is well illustrated by the fact that, as noted in Part One, section 2.1.5, of our submission,[3] 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.

This means that if the UK were to be granted a positive adequacy decision, personal data freely transferred to the UK under that decision could be freely onwardly transferred to that (in EU terms, not adequate) territory, Gibraltar, thus again undermining the protection of the EU GDPR and potentially creating yet another "data laundering haven".

4.3 Implications for the other "5EYES" (and other countries that indulge in mass surveillance)

The adequacy decisions on Canada (2001) and New Zealand (2012), like those on Guernsey, the Isle of Man and Jersey, were issued before the 2013 Snowden revelations about US, UK – and all the "5EYES" – surveillance operations. Therefore, the extensive cooperation between the intelligence agencies of those five countries was not considered in the context of those decisions. The fifth "5EYE", Australia, never received an adequacy decision.

[3] See also Part One, section 3.1, and footnote 25.

In our opinion, especially now that the only European member of the "5EYES", the UK, has left the EU, the data sharing arrangements between all the "5EYES" should be addressed in relation to all of them.

In our opinion , this means that the adequacy decisions on Canada and Australia, too, will have to be reviewed, also and especially taking into account the arrangements they have (mainly, under the UKUSA Agreement that has been extended to them) in relation to the sharing of intelligence data generally, and specifically the sharing of data extracted by any, some or all of them from Internet bearers. If, as we believe, the UK and the USA share, if not all then certainly much, of the data they extract from bearers – including such data on EU individuals as are included in those data – with Canada and New Zealand (and Australia), then the adequacy decisions on Canada and New Zealand, too, should be revoked or suspended, and Australian should not be granted one – until the "5EYES" all agree to bring their surveillance operations and laws in line with the European Essential Guarantees.

4.4 Implications for EU Member States

4.4.1 Implications for Member States' national security activities

A decision by the Commission to not issue a positive adequacy decision on the UK would not have any immediate legal implications for the EU Member States or the activities of their intelligence agencies – which would remain outside the scope of EU law.

However, if the decision not to issue a positive adequacy decision on the UK were to be based, at least in part, on the fact that the UK law and practices fail to meet the standards set by the CJEU in relation to third country agencies (as reflected in the European Essential Guarantees for surveillance issued by the EDPB), as presumably it would be – then the EU and its Member States could not avoid the accusation of hypocrisy and double standards. That is because several of them have laws and practices that also clearly do not meet those standards.[4]

Moreover, the intelligence agencies of several other EU Member States have been shown to have been cooperating with the US NSA in very much the same way as the UK (albeit as much more junior partners than the UK – often *de facto* little more than tools used by the NSA), including in the gathering of satellite communications[5] and tapping into underseas cables.[6]

It is long overdue that the EU – or at least, given the regrettable hole in the EU legal order when it comes to national security, the EU Member States – and other states that are

---

[4] Cf. the short country sections on France and Germany in Douwe Korff et al., Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes, January 2017, pp. 57 – 58 (and the references to these countries in the body of this report, *passim*), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894490

[5] "*Deutschland hat in enger Zusammenarbeit mit den amerikanischen Nachrichtendiensten über Jahrzehnte nicht nur mehr als 100 Staaten, darunter auch Freunde und Verbündete, belauscht.*" ("*For decades, Germany [read: the German Federal Intelligence Service, BND] has, in close cooperation with the American Intelligence Service [CIA] spied on more than 100 countries including friends and allies*"), in: "*Operation 'Rubikon' - #Cryptoleaks: Wie BND und CIA alle täuschten*" ("*Operation 'Rubikon' – How the BND and the CIA covered everything up*"), ZDF TV, 11 February 2020, available at: https://www.zdf.de/nachrichten/politik/cryptoleaks-bnd-cia-operation-rubikon-100.html

[6] *Danish military intelligence uses XKEYSCORE to tap cables in cooperation with the NSA*, Electrospaces, 28 October 2020, available at: https://www.electrospaces.net/2020/10/danish-military-intelligence-uses.html

supposed to be democracies that uphold and adhere to the Rule of Law, give serious attention to the urgent need to rein in their intelligence agencies. However, as noted in Part Two of our submission, until now only some tentative steps are being taken to adopt an international-legal framework for such agencies, such as the "intelligence codex" proposed by a former head of the German external intelligence service, the *Bundesnachrichtendienst* (BND), Mr Hansjörg Geiger (but even that was five years ago).[7]

It is notable that the European Data Protection Board, in its very recent recommendation on the kinds of "supplementary measures" that should be taken to protect personal data transferred from the EU to third countries, said that controllers and processors should adopt the same kinds of measures in relation to EU Member States (see the next sub-section).

In our opinion, the *Schrems II* judgment, the EDPB European Essential Guarantees, and the difficult issues raised in relation to the UK after Brexit, should now also urgently spur on the EU Member States to bring their own houses in order in relation to mass surveillance and bulk collection of personal data including (but far from limited to) communications metadata.

4.4.2 Implications for EU controllers and processors

Finally, we should note that any decision by the European Commission to not issue a positive adequacy decision on the UK would have major implications for EU-based controllers and processors of personal data. Specifically, they will have to go through all the steps outlined in the EDPB recommendation on "supplementary measures" that will have to be adopted in relation to transfers of personal data to the UK after 1 January 2021, including close study of the UK's surveillance law and practices (in which our submission and the references in it may be helpful); the adoption of such measures (very strong encryption; limiting transfers to fully anonymised or very strongly pseudonymised data; strong contractual stipulations); informing of and consultation with their national data protection supervisory authority in relation to any doubts as to whether the data that are to be transferred can be effectively protected against the activities of the UK GCHQ (and the US NSA); and ending or not commencing transfers to the UK if protection cannot be effectively achieved.

Failure to carry out these tasks, and failure to protect the data against bulk extraction by GCHQ, would be a breach of the GDPR – and, in our opinion, would constitute a personal data breach for which the EU-based data exporter will be liable.[8] In other words, failure, not just by the EU institutions but also by individual EU-based controllers and processors to take the matters we discussed in our submission seriously, will have major repercussions.

EU-based controllers and processors who fail to serious study the surveillance law and practices of the UK, and to protect any data they transfer to the UK after the post-Brexit transition period against GCHQ interception, will be exposed to serious administrative fines under the GDPR (for breaches of the transfer regime in Chapter V) and to liability for payment of damages to data subjects – who can now demand such damages also in representative actions.

- o – O – o -

7 See Part Two, section 2.2.1, footnote 7.

8 See Part Two, section 3.1.3.i.