The Implications of a 'No-Deal' Brexit for Data Protection in the UK

Dr Oliver Butler[i]

Abstract: A 'No-deal' Brexit will have important implications for international data transfers from the EU to the UK. It will both impose costs on and harm the competitiveness of many UK-based companies. However, a sharp "cliff-edge" for international data flows is less likely. UK-based companies will need to rely on Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) for international data transfers from the EU in the event of 'a No-deal' Brexit. Many larger companies are likely to have already taken steps towards implementing such measures. In addition, very considerable progress has been made by the UK and third countries with EU adequacy decisions in their favour to ensure that international data flows are maintained.

The most significant implication of a 'No-deal' Brexit is in the medium term. A 'No-deal' Brexit makes it more likely that any attempt to seek an EU adequacy decision for future international data transfers for the UK will fail. This increases the prospect of weakening existing protections for the personal data of UK-resident data subjects both in the UK and abroad and in both the public and private sectors.

Keywords: 'No-deal' Brexit; International Data Transfers; Adequacy Decisions.

Author Description: Dr Oliver Butler is a Research Fellow of the Bonavero Institute of Human Rights and a Fellow of Wadham College, University of Oxford. His research interests cover the changing application of data protection, privacy and confidentiality to the public and private sectors, both within and beyond the EU. The Bonavero Institute of Human Rights is a research institute of the Faculty of Law, University of Oxford, which undertakes world-class research in the field of human rights law and fosters public engagement in human rights issues beyond the academy.

Introduction

At the time of writing, the UK is due to leave the EU on 31st October 2019 and the UK Government is committed to leave with or without a withdrawal agreement (a 'No-deal' Brexit'). The prospect of a 'No-deal' Brexit is higher than ever. What is at stake for data protection in the event of a 'No-deal' Brexit? This article assesses the short and medium term implications of a 'No-deal' Brexit for data protection in the UK and argues that the medium term implications are of greatest significance. It does this by considering the effect of a 'No-deal' Brexit on international data transfers in the event of a 'No-deal' Brexit, the prospects of an EU adequacy decision following a 'No-deal' Brexit, and the possible scope of UK divergence in data protection laws. Understanding those implications can help us to clarify what is at stake in securing a withdrawal agreement, to understand the prospect of UK divergence from EU data protection standards both with and without a deal, and to act to preserve international data flows in the event of a 'No-deal' Brexit. As Patel and Lee observe, the impact of Brexit on data flows has received little attention in Brexit debates.[ii]

A ‘No-deal’ Brexit has significant implications for international data transfers from the EU to the UK, imposing costs on, and harming the competitiveness of, many UK-based companies. However, a sharp “cliff-edge” for international data flows is unlikely. Very considerable progress has also been made by the UK and third countries with EU adequacy decisions in their favour to ensure that international data flows are maintained in the event of a ‘No-deal’ Brexit. UK-based companies will need to rely on Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) for international data transfers from the EU in the event of ‘a No-deal’ Brexit. Indeed, it is likely that many major companies have already put such provisions in place, in the run up to the earlier 29th March 2019 deadline, which highlighted the increasing risk of a ‘No-deal’ Brexit. Disruption is more likely to be felt among small and medium enterprises (SMEs), new data transfers, and arrangements where the value of the UK market to an EU controller’s or processor’s business does not outweigh the increased cost of putting in place adequate safeguards. The territorial scope of the General Data Protection Regulation (GDPR) and retention of data protection laws in the UK GDPR post-Brexit mean that there will be little other change in data protection law in the short term in the UK.

In the medium term, it is likely that the UK will seek an EU adequacy decision for international data transfers from the EU to the UK, as it would have done under the 25th November 2019 Withdrawal Agreement and Political Declaration. However, a ‘No-deal’ Brexit differs from the Withdrawal Agreement in two important respects. First, the Withdrawal Agreement would have bound the UK closely to EU data protection laws and so reduce the scope for post-Brexit divergence, both legally and practically. Second, the absence of a transition period in a ‘No-deal’ Brexit means that much of the feared cost and disruption of leaving without an adequacy decision will be realised before any adequacy decision can be made.

These factors are both important because there are aspects of GDPR that will be seen by its opponents as attractive areas for divergent approaches by the UK post-Brexit. This is particularly true of data processing by public authorities, reducing the regulatory burden on SMEs, and facilitating international data transfers from the UK to third countries that do not have EU adequacy decisions. This, combined with heightened scrutiny of UK surveillance and other legislation during adequacy assessments by and negotiations with the EU Commission, with possible pressures for reform, may yet work to result in the failure of the attempt to gain an EU adequacy decision. This is the more serious implication of a ‘No-deal’ Brexit, increasing the prospect of weakening existing protections for the personal data of UK-resident data subjects in both the public and private sectors and in both the UK and abroad.

The Implications for International Data Transfers following a ‘No-deal’ Brexit

Following a ‘No-deal’ Brexit the UK will leave the EU become a third country for the purposes of GDPR.[iii] There are six types of international data transfer that are potentially affected by a ‘No-deal’ Brexit: transfers from the EU/EEA to the UK, transfers from the UK to the EU/EEA, transfers from the UK to a third country with an EU Commission adequacy decision in its favour, transfers from a third country with an EU Commission adequacy decision to the UK, transfers from the UK to a third country without an EU Commission adequacy decision, and transfers from a third country without an EU Commission adequacy decision to the UK. Of these, there are only significant implications for transfers from the EU to the UK, as a result of recent legislative and other changes in the UK and by most third countries with EU Commission adequacy decisions in their favour.

International transfers from the EU to UK

Under the GDPR, personal data transfers to a third country may only take place if one of the conditions in Articles 45 to 49 GDPR are complied with by the controller and processor.[iv] This includes onward transfer from the third country to another third country or an international organisation.[v] These rules are required to be "applied in order to ensure that the level of protection of natural persons guaranteed by [the GDPR] is not undermined" by data transfers to third countries with lower levels of data protection.[vi]

Data transfers to a third country may take place where the EU Commission has decided that the third country ensures "an adequate level of protection".[vii] Such transfers do not require "any specific authorisation".[viii] In C-362/14 *Schrems v Data Protection Commissioner*,[ix] the Grand Chamber of the Court of Justice of the European Union (CJEU) held that "an adequate level of protection" must be understood "as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is *essentially equivalent* to that guaranteed within the European Union".[x]

However, the UK will not have an EU adequacy decision in its favour on Brexit day. On 13th September 2018, the Department for Digital, Culture, Media and Sport (DCMS) noted that: "while we have made it clear we are ready to begin preliminary discussions on an adequacy assessment now, the European Commission has not yet indicated a timetable for this and have stated that the decision on adequacy cannot be taken until we are a third country."[xi] The UK Information Commissioner Elizabeth Denham has warned that as "an assessment of adequacy can only take place once the UK has left the EU" and the necessary assessments and negotiations 'have usually taken many months",[xii] there will not be an EU adequacy decision in place following a No-deal Brexit.

International data transfers from the EU to the UK will therefore have to rely on Article 46 GDPR safeguards or Article 49 GDPR derogations. A controller or processor may transfer personal data to a third country under Article 46 GDPR only if the controller has "provided appropriate safeguards" and "on condition that enforceable data subject rights and effective legal remedies for data subjects are available".[xiii] Without any specific authorisation from a supervisory authority, appropriate safeguards may be provided for by SCCs adopted by the Commission[xiv] or BCRs.[xv] Competent supervisory authorities must approve BCRs in accordance with the consistency mechanism provided for by the GDPR, provided that those BCRs "are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees" and "expressly confer enforceable rights on data subjects with regard to the processing of their personal data".[xvi]

The European Dara Protection Board (EDPB) recommends SCCs as a "ready-to-use instrument".[xvii] Information Commissioner's Office (ICO) Guidance observes that SCCs are "most likely to be appropriate for small and medium-sized businesses" for transfers outside the EEA by an EU controller, although there are no approved SCCs for transfers outside the EEA by a processor within the EU.[xviii] It recommends agreeing SCCs with an EU controller. The European Commission has only published SCCs for EU controller to non-EU controller and EU controller to non-EU processor.[xix]

There is some uncertainty about the legality of international data transfers to third countries using SCCs. C 311/18 *Data Protection Commissioner v Schrems ("Schrems II")* is a reference for a preliminary ruling from the High Court in Ireland to determine whether "there is a violation of the rights of an individual through the transfer of data from the EU to a third country under the SCC Decision where it may be further processed for national security purposes".[xx] These concerns arise from the wide surveillance powers exercised by authorities in the USA. The CJEU heard the case on 9th July 2019. The Advocate General Opinion is expected on 12th December 2019 and the full decision in early 2020, so the uncertainty cannot be resolved before Brexit. If the CJEU takes a restrictive approach, SCCs to the UK may be affected.

The EDPB points to some of the complexities of seeking BCRs in anticipation of Brexit.[xxi] It recommends that groups headquartered in the UK should identify the "most appropriate BCR Lead supervisory Authority in a EU Member State" if they wish to apply for BCR. If BCRs are at review stage by the ICO, the group will need to "identify a new BCR Lead Supervisory Authority… [who] will take over the application and formally initiate a new procedure at the time of a no deal Brexit" and "if a draft ICO decision for approving BCRs is pending before the EDPB at the time of a No-deal Brexit, the Group needs to identify a new BCR Lead Supervisory Authority. The new BCR Lead will take over and re-submit a draft decision for the approval the BCRs to the EDPB." Current holders of authorised BCRs will "need to identify the new BCR Lead Supervisory Authority". Brexit has the potential to disrupt and complicate the process of approving new BCRs.

Where a group already has EEA approved BCRs in place, the ICO recommends updating those rules, their documentation and privacy notices to "reflect that, under the EU GDPR, the UK becomes a third country" after Brexit.[xxii] UK-based controllers must also appoint a representative within the EU. As the ICO notes, the "view of the EDPB is that supervisory authorities are able to initiate enforcement action (including fines) against a representative in the same way as they could against the controller or processor which appointed them."[xxiii] Given that the role is potentially burdensome, UK-based controllers may find that appointing a representative is challenging and expensive.

Although Article 46 GDPR also makes provision for SCCs adopted by a supervisory authority and approved by the Commission,[xxiv] codes of conduct,[xxv] and certification mechanisms to provide appropriate safeguards,[xxvi] none of these mechanisms have yet been set up and it is unlikely that they will be available and functioning by 31st October 2019.[xxvii]

Finally, where SCCs or BCRs are not in place, derogations under Article 49 GDPR permit transfers from the EU where the data subject has:

- explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;[xxviii]

- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;[xxix]
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;[xxx]
- the transfer is necessary for important reasons of public interest;[xxxi]
- the transfer is necessary for the establishment, exercise or defence of legal claims;[xxxii]
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;[xxxiii]
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.[xxxiv]

Such transfers cannot be repetitive, must only concern a limited number of data subjects and must be necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interest or rights and freedoms of the data subject.[xxxv] The controller must also assess all the circumstances surrounding the data transfer and provide "suitable safeguards with regard to the protection of personal data".[xxxvi] Additionally, the controller must inform the supervisory authority of the transfer and inform the data subject of the transfers and the compelling legitimate interests pursued.[xxxvii] Derogations are therefore burdensome and may only play a relatively limited role in international data transfers.

Ensuring that all controllers have in place SCCs or BCRs for transfers from the EU to the UK represents a considerable administrative burden on UK businesses and their EU partners. It is reasonable to expect that some controllers will fail to put in place appropriate safeguards and so some international transfers will be disrupted or occur in breach of GDPR. It will also affect the competitiveness of UK-based companies, by imposing additional burdens on international transfers to the UK. It is difficult to evaluate how large the economic impact of putting in place SCCs or BCRs will be but it is undoubtedly a substantial task imposed on the private sector.[xxxviii]

Patel and Lee argue that it is "likely that many firms will not be ready".[xxxix] This is certainly true of SMEs. However, a sharp "cliff-edge" for international data flows is unlikely for many larger companies.[xl] Uncertainty surrounding the risk of a 'No-deal' Brexit and the commitment of the Government to leave with or without a deal on 31st October 2019 mean that preparations for appropriate safeguards to apply from 31st October 2019 will occur in advance of exit day. Indeed, many major UK-based companies will already have taken such steps in the run up to the 29th March 2019 deadline, to protect themselves in the event of the UK crashing out without an extension at that time. The greatest impact is likely to be on new data transfer arrangements, unprepared SMEs, or EU controllers and processors who are unwilling to meet the costs of data transfers to the UK, if for example the UK market is not a significant part of their business.

International Transfers from the UK to the EU and 'Adequate' Third Countries

International transfers to the EU and 'adequate' third countries from the UK will be unaffected in the event of a 'No-deal' Brexit. DCMS guidance explains that the UK will "transitionally recognise all EEA countries (including EU Member States) and Gibraltar as 'adequate' to allow data flows from the UK to Europe to continue" and "preserve the effect of existing EU adequacy decisions on a transitional basis".[xli]

Amendments made to the Data Protection Act 2018 by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 made pursuant to the EU (Withdrawal) Act 2018 will empower the Secretary of State to make regulations specifying that a third country ensures an "adequate level of protection of personal data"[xlii] for the purposes of transfers under the UK GDPR. Article 45(2) UK GDPR preserves the same criteria as those which apply to EU Commission adequacy decisions.[xliii] The Secretary of State is required to review the level of protection at least every 4 years,[xliv] taking into account all relevant developments,[xlv] to monitor developments, [xlvi] and, if the level is no longer adequate, to amend or revoke the regulations and "enter into consultations with the third country or international organisation concerned with a view to remedying the lack of an adequate level of protection".[xlvii] These UK adequacy regulations are "subject to the negative resolution procedure".[xlviii] There is therefore a significant risk that they will only receive very limited parliamentary oversight but little risk that they will not be in place by 31st October 2019.

International Transfers from 'Adequate' Third Countries to the UK

Of the third countries with EU adequacy decisions in their favour, Argentina,[xlix] Canada,[l] Faroe Islands,[li] Guernsey,[lii] Isle of Man,[liii] Israel,[liv] Japan,[lv] Jersey,[lvi] New Zealand,[lvii] Switzerland,[lviii] United States of America,[lix] and Uruguay[lx] have all put in place national provisions or changes that permit transfers from the third country to the UK. The only apparent exception is Andorra, for which there is no current information.[lxi] There will therefore be very limited implications for international transfers from 'adequate third countries to the UK, even in the event of a 'No-deal' Brexit.

International Transfers from the UK to Other Third Countries

Transfers to other third countries, currently under Article 46 and 49 GDPR, will continue in much the same way post-Brexit. DCMS guidance explains that the UK will recognise EU SCCs in UK law, give the ICO power to issue new clauses, and recognise BCRs authorised before exit day.[lxii] Amendments made to the Data Protection Act 2018 by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 made pursuant to the EU (Withdrawal) Act 2018 empower the Secretary of State to make regulations to specify standard data protection clauses which provide appropriate safeguards for the purposes of Article 46 UK GDPR international transfers.[lxiii] These must be kept under review[lxiv] and are also subject to the negative resolution procedure.[lxv] The ICO may also "issue a document specifying standard data protection clauses which the Commissioner considers provide appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Article 46 of the UK GDPR".[lxvi]

International Transfers from Other Third Countries to the UK

Many countries place restrictions on international transfers of personal data. Although this is unaffected by Brexit, the UK may lose the benefit of any recognition granted to the EU as a whole by other third country transfer regimes and so companies should be alive to this risk and put in place suitable arrangements to satisfy other third countries' international data transfer rules.

Continued Compliance with Data Protection Laws after Brexit

There will be little other change to data protection law applicable in the UK in the immediate aftermath of a 'No-deal' Brexit. GDPR will be retained law pursuant to the European Union (Withdrawal) Act 2018, subject to changes made by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019. The majority of those changes relate to changing references to Union law to domestic law, the European Commission to the Secretary of State, the supervisory authority to the Information Commissioner, and removing references to the EU cooperation and consistency mechanisms that the UK will no longer participate in post-Brexit.

In any case, even once the UK is outside the EU, much UK-based data processing will still fall within the territorial scope of the EU GDPR. GDPR applies to personal data processing "in the context of an establishment of a controller or processor in the Union, regardless of whether the processing takes place in the Union or not".[lxvii] It is notable that this is already broader than the territorial scope of the equivalent provision in the Data Protection Directive 95/46/EC, which only applied to processing "in the context of an establishment of a controller".[lxviii]

This is important because the use of an EU-established processor can be sufficient to bring processing within the scope of GDPR. The Grand Chamber of the CJEU interpreted "in the context of an establishment… in the Union", in Article 4(1)(a) Directive 95/46/EC, broadly in C-131/12 *Google Spain SL v AEPD*.[lxix] The Grand Chamber held that processing "carried out in the context of the activities" of Google Spain, which was established in Spain to promote and sell advertising space on behalf of Google Search, included the search indexing of Google Inc., as they were "inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that the engine is, at the same time, the means enabling those activities to be performed".[lxx]

GDPR also applies to the processing of personal data or data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the "offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union"[lxxi] or the "monitoring of their behaviour as far as their business takes place within the Union".[lxxii]

Many UK-based companies will therefore need to comply with both the GDPR and the UK GDPR post-Brexit. An important implication of this is that such organisations will need to identify their new Lead Supervisory Authority within the EU, update their privacy notices accordingly, and appoint EU representatives.

Prospects of an EU Adequacy Decision for the UK following a 'No-deal' Brexit

The UK is likely to seek an adequacy decision whether Brexit is based on a deal or 'No-deal'.[lxxiii] However, a 'No-deal' Brexit increases the possibility that the attempt to receive an adequacy decision will be abandoned by the UK . This could lead to more significant divergence in the medium to long term.

The Withdrawal Agreement would have done much to bind the UK legally and practically to EU data protection standards. The Withdrawal Agreement provided for data protection post-Brexit in Title VII. Title VII would have required the UK to continue to maintain data protection laws broadly in line with EU data protection law for much personal data. Article 71(1) WA provided for "Union law on the protection of personal data"[lxxiv] to apply in the United Kingdom in respect of the processing of personal data of data subjects "outside the United Kingdom" provided that the personal data "were processed under Union law in the United Kingdom before the end of the transition period" or "are processed in the United Kingdom after the end of the transition period on the basis of [the Withdrawal Agreement]". This would cease to be the case "to the extent the processing of the personal data… is subject to an adequate level of protection as established in applicable decisions under Article 45(3) of Regulation (EU) 2016/679 or Article 36(3) of Directive (EU) 2016/680".[lxxv] However, if such adequacy decisions ceased to be applicable, the UK would still be obliged to "ensure a level of protection of personal data *essentially equivalent* to that under Union law" for the protection of personal data in respect of the processing of personal data covered by Article 71(1) WA.[lxxvi]

Essential equivalence to Union law is of course the test for an adequacy decision under EU law[lxxvii] and so, whether recognised as adequate or not, the UK would be bound closely to EU data protection law for data subjects outside the UK whose data was processed before Brexit. This would greatly have reduced the appeal of future UK divergence, due to the practical difficulties of implementing different data protection standards in pre-Brexit databases with a mixture of UK-resident and non-resident data subjects.

The Political Declaration emphasised the "importance of data flows and exchanges across the future relationship" [lxxviii] and the commitment of both Parties to "ensuring a high level of personal data protection to facilitate such flows between them."[lxxix] The European Commission would "start the assessments with respect to the United Kingdom as soon as possible after the United Kingdom's withdrawal, endeavouring to adopt decisions by the end of 2020, if the applicable conditions are met".[lxxx] The UK would "in the same timeframe take steps to ensure the comparable facilitation of transfers of personal data to the Union, if the applicable conditions are met".[lxxxi] Had international data transfers been preserved during a transition period and an adequacy decision made before it ended, the implications for EU to UK transfers discussed above could have been avoided.

Despite the fact that the Political Declaration added that the "future relationship will not affect the Parties' autonomy over their respective personal data protection rules",[lxxxii] it would have done much to limit the practical likelihood of post-Brexit divergence in data protection laws by incentivising the UK to take any necessary steps to gain and maintain adequacy. However, if a 'No-deal' Brexit occurs, the economic incentive to seek and maintain adequacy will be reduced because many costs of putting in place alternative adequate safeguards will be realised before adequacy is sought.

Other factors also place an EU adequacy decision in doubt. Article 45(2) GDPR requires the EU Commission to take into account a number of elements when assessing the adequacy of the level of protection offered by a third country. These elements include, importantly, "relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data" and the implementation of such legislation.[lxxxiii]

This will mean that the legislative powers of UK public authorities will come under much greater scrutiny than would be the case within the EU, where individual laws may be challenged in courts or doubted by regulators but are not systematically reviewed. The scrutiny of the EU Commission would be ongoing. The EU Commission must carry out periodic reviews of its adequacy decisions, at least every four years, taking into account relevant developments in the third country,[lxxxiv] and monitor developments that could affect the functioning of its decisions on an ongoing basis,[lxxxv] so that where the available information reveals that a third country "no longer ensures an adequate level of protection" it must, "to the extent necessary, repeal, amend or suspend the decision".[lxxxvi] Such a repeal, amendment or suspension must be followed by "consultations with the third country… with a view to remedying the situation giving rise to the decision".[lxxxvii]

There are concerns, in particular, that the UK's extensive surveillance laws, exempt from the scope of GDPR while a Member State,[lxxxviii] which will come under close scrutiny once it is a third country seeking adequacy.[lxxxix] Patel and Lea report that interviews with EU and UK politicians, civil servants, lawyers, and other professionals reveal widespread concern about the UK's prospects of securing an adequacy decision.[xc] They explain that the intrusive surveillance powers in the Investigatory Powers Act 2016, the UK's participation in the Five Eyes intelligence sharing arrangement between the UK, US, Australia, Canada and New Zealand, the UK's failure to retain the fundamental right to data protection from the EU Charter of Fundamental Rights, potential future onwards data transfers from the UK to countries without EU adequacy decisions, and the immigration exemption in the Data Protection Act 2018 all risk the UK's ability to secure an adequacy decision from the European Commission.[xci] They conclude that "the path to adequacy will be turbulent at best" and will be challenged in the courts.[xcii]

It is difficult to predict how the European Commission will view such issues, whether it will demands reforms, and whether an adequacy decision would survive review by the CJEU. To obtain adequacy post-Brexit, the UK may be required to strengthen its data protection laws beyond the level required as a Member State, especially in relation to national security. One could certainly imagine UK politicians strongly resisting a perceived attempt by the EU Commission to impose reforms on the UK laws concerning national security. This could lead to the UK abandoning the attempt to gain adequacy.

Adequacy decisions adopted by the EU Commission on the basis of Article 25(6) of Directive 95/46/EC remain in force until amended, replaced or repealed by Article 45 GDPR adequacy decisions.[xciii] Therefore the adequacy decisions relating to Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework), will all come under review, subject to the higher standard of essential equivalence under GDPR. The UK will no doubt watch with interest the reviews of existing adequacy decisions for alternative models of data protection that are considered by the EU Commission to provide an adequate level of protection. In particular, it might question whether a narrower adequacy decision for the private sector only, as in Japan under the GDPR, might be a more attractive model.[xciv]

The Scope for Divergence following a 'No-deal' Brexit without an Adequacy Decision

Even in the event of a 'No-deal' Brexit and if the UK abandoned adequacy standards, the UK would nevertheless continue to be a signatory of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)[xcv] and the European Convention on Human Rights, notably including Article 8 ECHR, the right to private life. Although these place some limits on the extent to which the UK can diverge from EU data protection law, many countries do maintain different data protections laws while signatories to these treaties. They do both create a "floor" of data protection rights, however, below which the UK could not go without revisiting its relationship to those treaties. Within this, there are three key areas where the UK might seek to "take advantage of Brexit" in the field of data protection.[xcvi]

First, some might seek to reduce restrictions on public authorities' data processing. Public authorities do not usually have EU establishments, offer services to data subjects in the Union or monitor the behaviour of data subjects in the Union. They will not therefore easily fall within the scope of the EU GDPR post-Brexit, if they avoid processing with EU-established controllers or processors, making divergence a practical possibility. One of the changes brought about by GDPR was the loss of "legitimate interests" as a ground for processing by public authorities.[xcvii] Although the Data Protection Act 2018 section 7(2) seeks to mitigate this by providing that a public authority as defined by section 7(1) is "only a 'public authority' or 'public body' for the purposes of the GDPR when performing a task carried out in the public interest or in the exercise of official authority vested in it",[xcviii] there may be appetite to return to the more generous position for public authorities under Directive 95/46/EC. More generally, there might be an appetite to reduce restrictions on public authority data processing and the regulatory burdens they face, subject to Convention 108 and Article 8 ECHR. Notably, Japan's recent adequacy decision was limited to "Personal Information Handling Business Operators" and excluded central and local government and administrative agencies, suggesting such a possibility exists.[xcix]

Second, although many UK-based companies will fall within the broad territorial scope of GDPR and comply with it across their data processing activities,[c] there are likely to be businesses in some sectors, especially SMEs, that do not fall within the scope of GDPR and see advantage in reducing the regulatory burden of data protection laws in the UK. There might also be pressure to reduce the burden of data protection laws to encourage tech start-ups and collaboration with partners in non-EEA markets.

Third, if the UK was neither bound by the Withdrawal Agreement nor seeking to maintain an adequacy decision in its favour, it would be easier for the Secretary of State to make adequacy regulations in favour of other third countries more quickly that the EU Commission. For some, this would overcome the disadvantages of the cumbersome EU process and long queue of adequacy applicants, allowing the UK to promote data transfers to other countries and steal a march on the EU by establishing stronger relationships with data controllers and processors in third countries. Although this undoubtedly has its risks depending on the rigour of UK assessments, the independence of the Secretary of State, willingness of the UK courts to review such decisions, and the difficulties of achieving sufficient parliamentary scrutiny through the negative resolution procedure in Parliament, it will likely be attractive to politicians keen to promote "Global Britain" and international trade.

Conclusion

Many advocates of data protection and privacy would undoubtedly view such a vision of UK divergence from European Union data protection law with horror, as weakening protections for UK data subjects in both the public and private sectors and in both the UK and abroad. The erosion of the UK's economic and legal reasons for maintaining essential equivalence with EU data protection standards in the medium term is the most important implication of a 'No-deal' Brexit for UK data protection law. Although UK-based companies will need to make sure that they have put in place the appropriate safeguards necessary to preserve international data transfers from the EU to the UK post-Brexit with their EU partners, and this will impose costs and damage UK-competitiveness within the EU in ways that could have been avoided through the Withdrawal Agreement, such short-term implications pale against this more significant implication of a 'No-deal' Brexit to UK data protection law.

---

[i] Research Fellow, Bonavero Institute of Human Rights, University of Oxford. Fellow, Wadham College, University of Oxford. This article builds on my conference presentation *"Tensions between the UK and GDPR after Brexit"* at the 31st Annual Privacy Laws and Business International Conference and comments on the 32nd Annual Privacy Laws and Business International Conference in Oliver Butler, *The UK's Room for Manoeuvre in Data Protection Legislation after Brexit* (2019) 104 PLB 12. I am grateful to attendees at both conferences for their comments and discussions, in particular Dr David Erdos and Stewart Dresner, and to the anonymous reviewer of this article. Any errors or omissions are my own.

[ii] Oliver Patel and Nathan Lee, EU-UK Data Flows, Brexit and No-deal: Adequacy or Disarray? UCL European Institute Brexit Insights (August 2019), p. 7.

[iii] EDPB, *Information Note on Data Transfers under the GDPR in the Event of a No-Deal Brexit* (12th February 2019): https://edpb.europa.eu/our-work-tools/our-documents/drugo/information-note-data-transfers-under-gdpr-event-no-deal-brexit_en.

[iv] Article 44 GDPR.

[v] *Ibid.*

[vi] *Ibid.*

[vii] *Ibid.*

[viii] *Ibid.*

[ix] ECLI:EU:C:2015:650.

[x] *Ibid.*, para. 73 (emphasis added).

[xi] DCMS, *Data Protection if there's no Brexit Deal*, https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal.

[xii] Elizabeth Denham, *Blog: How will personal data continue to flow after Brexit?*, https://ico.org.uk/about-the-ico/news-and-events/blog-how-will-personal-data-continue-to-flow-after-brexit/.

[xiii] Article 46(1) GDPR.

[xiv] Article 46(2)(c) GDPR.
[xv] Article 46(2)(b) GDPR.
[xvi] Article 47 GDPR.
[xvii] EDPB, *Information Note Data Transfers under GDPR in the Event of a No Deal Brexit* https://edpb.europa.eu/our-work-tools/our-documents/drugo/information-note-data-transfers-under-gdpr-event-no-deal-brexit_en.
[xviii] ICO, *How to Transfer Data from Europe to the UK using SCCs* https://ico.org.uk/for-organisations/data-protection-and-brexit/how-to-transfer-data-from-europe-from-the-eea-to-the-uk-using-standard-contractual-clauses-sccs/.
[xix] See European Commission, *Standards Contractual Clauses* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.
[xx]C 311/18 *Data Protection Commissioner v Schrems* http://curia.europa.eu/juris/document/document.jsf?text=&docid=204046&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6462885.
[xxi] EDPB, Information Note on BCRs for Companies which have ICO as BCR Lead Supervisory Authority https://edpb.europa.eu/our-work-tools/our-documents/other/information-note-bcrs-companies-which-have-ico-bcr-lead_en.
[xxii] ICO Guidance, *Data Protection if there's no Brexit deal*, https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-there-s-no-brexit-deal/.
[xxiii] *Ibid.*
[xxiv] Article 46(2)(d) GDPR.
[xxv] Article 46(2)(e) GDPR.
[xxvi] Article 46(2)(f) GDPR.
[xxvii] ICO, *Guide to the GDPR: International Transfers* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/.
[xxviii]Article 49(1)(a) GDPR.
[xxix] Article 49(1)(b) GDPR.
[xxx] Article 49(1)(c) GDPR.
[xxxi] Article 49(1)(d) GDPR.
[xxxii] Article 49(1)(e) GDPR.
[xxxiii] Article 49(1)(f) GDPR.
[xxxiv] Article 49(1) (g) GDPR.
[xxxv] Article 49(1) GDPR.
[xxxvi] *Ibid.*
[xxxvii] *Ibid.*
[xxxviii] Patel and Lee, EU-UK Data Flows, Brexit and No-deal: Adequacy or Disarray? UCL European Institute Brexit Insights (August 2019), pp. 10 to 11.
[xxxix] *Ibid.*, p. 11.
[xl] Whether a 'No-deal' Brexit will result in a broader economic cliff-edge is outside the scope of this paper.
[xli] DCMS, *Amendments to UK Data Protection Law in the Event the UK Leaves the EU without a Deal on 29 March 2019* https://www.gov.uk/government/publications/data-protection-law-eu-exit/amendments-to-uk-data-protection-law-in-the-event-the-uk-leaves-the-eu-without-a-deal-on-29-march-2019.
[xlii] *Ibid.*, s. 17A(1).
[xliii] *Ibid.*, s. 17A(4).
[xliv] *Ibid.*, s. 17B(1).
[xlv] *Ibid.*, s. 17B(2).
[xlvi] *Ibid.*, s. 17B(3).
[xlvii] *Ibid.*, ss. 17(B)(4) and (5).
[xlviii] *Ibid.*, s. 17A(7).
[xlix] https://www.boletinoficial.gob.ar/detalleAviso/primera/202373/20190226.
[l] http://www.ic.gc.ca/eic/site/113.nsf/eng/07665.html.
[li] http://dat.fo/00003/00157/.
[lii] http://www.guernseylegalresources.gg/article/170185/Data-Protection-Authorised-Jurisdiction-Bailiwick-of-Guernsey-Ordinance-2019.
[liii] http://www.tynwald.org.im/business/opqp/sittings/20182021/2019-SD-0139.pdf.

[liv] https://www.gov.il/BlobFolder/legalinfo/legislation/en/PrivacyProtectionTransferofDataabroadRegulationsun.pdf.
[lv] https://www.ppc.go.jp/files/pdf/310315_houdou.pdf.
[lvi] https://www.jerseylaw.je/laws/enacted/Pages/RO-009-2019.aspx.
[lvii] https://www.mfat.govt.nz/en/countries-and-regions/europe/united-kingdom/brexit-the-uk-and-europe/.
[lviii] https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html.
[lix] https://www.privacyshield.gov/article?id=Privacy-Shield-and-the-UK-FAQs.
[lx] https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-42019.
[lxi] Search of the Andorra Data Protection Agency website for "Brexit" returns no results.
[lxii] DCMS, *Amendments to UK Data Protection Law in the Event the UK Leaves the EU without a Deal on 29 March 2019* https://www.gov.uk/government/publications/data-protection-law-eu-exit/amendments-to-uk-data-protection-law-in-the-event-the-uk-leaves-the-eu-without-a-deal-on-29-march-2019.
[lxiii] Data Protection Act 2018, s. 17C(1).
[lxiv] *Ibid.*, s. 17C(2).
[lxv] *Ibid.*, s. 17C(3).
[lxvi] *Ibid.*, s. 119A.
[lxvii] Article 3(1) GDPR.
[lxviii] Article 4(1)(a) Directive 95/46/EC. Note that Directive 95/46/EC also applied to the processing of personal data where "the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory though the territory of the Community": Article 4(1)(c) Directive 95/46/EC.
[lxix] ECLI:EU:C:2014:317.
[lxx] *Ibid.,* para. 56.
[lxxi] Article 3(2)(a) GDPR
[lxxii] Article 3(2)(b) GDPR. GDPR also applies to the processing of personal data by a controller bot established in the Union, but in a place where Member State law applies by virtue of public international law: Article 3(3) GDPR.
[lxxiii] See Oliver Butler, *The UK's Room for Manoeuvre in Data Protection Legislation after Brexit* (2019) 104 PLB 12.
[lxxiv] This was defined by Article 70 WA to include Regulation (EU) 2016/679, with the exception of Chapter VII thereof, Directive (EU) 2016/680; Directive 2002/58/EC and "any other provisions of Union law governing the protection of personal data".
[lxxv] Article 71(2) WA.
[lxxvi] Article 71(3) WA (emphasis added).
[lxxvii] See above p. 3.
[lxxviii] Political Declaration setting out the Framework for the Future Relationship between the European Union and the UK (25 November 2018) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759021/25_November_Political_Declaration_setting_out_the_framework_for_the_future_relationship_between_the_European_Union_and_the_United_Kingdom__.pdf.
[lxxix] *Ibid.*, para. 8.
[lxxx] *Ibid.* para. 9.
[lxxxi] *Ibid.*
[lxxxii] *Ibid.*
[lxxxiii] Article 45(2)(a) GDPR.
[lxxxiv] Article 45(3) GDPR.
[lxxxv] Article 45(4) GDPR.
[lxxxvi] Article 45(5) GDPR.
[lxxxvii] Article 45(6) GDPR.
[lxxxviii] Article 2(2) GDPR.
[lxxxix] For a good explanation of the issues, see Andrew D. Murray, *Data Transfers between the EU and UK post Brexit?* (2017) 7(3) International Data Privacy Law 149.
[xc] Patel and Lee, EU-UK Data Flows, Brexit and No-deal: Adequacy or Disarray? UCL European Institute Brexit Insights (August 2019), p. 9.

[xci] *Ibid.*, pp. 10 and 11.
[xcii] *Ibid.*, p. 11.
[xciii] Article 45(9) GPDR.
[xciv] See below, p. 10.
[xcv] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.
[xcvi] Boris Johnson, *Speech on the Steps of No. 10 Downing Street* (24.07.2019).
[xcvii] Contrast Article 6 GDPR with Article 7 Directive 95/46/EC.
[xcviii] See Oliver Butler, *Obligations Imposed on Private Parties by the GDPR and UK Data Protection Law: Blurring the Public-Private Divide* (2018) 24(3) EPL 555.
[xcix] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, paras 10 and 32.
[c] See above p. 7.