

**REPORT OF THE AGMA DPA/FoIA COORDINATOR**

Date: 8th January 2019

**1.0 Purpose of report:**

1.1 This report:

* reviews the preliminary ruling of the Court of European Justice (CJEU) on a reference (originating from the Scottish Court of Sessions) finding that a Member State may unilaterally revoke an Article 50 notice to withdraw from the EU, prior to its expiry;
* explains the general data protection implications of the UK leaving with EU with an agreed Withdrawal Agreement or on the basis of ‘no deal’ scenario;
* reviews the guidance recently issued by the DCMS and the Information Commissioner explaining the impact that a no-deal Brexit scenario will have, including steps that organisations can take to prepare for that possibility;
* provides an overview of the contingency legislation the Government has laid before Parliament which will create a new version of the GDPR in UK law (to be known as the ‘UK GDPR’) in the event that ‘no deal’ is the basis for the UK’s departure from the EU on 29th March 2019;
* identifies minimum measures that Councils need to urgently take to identify data flows with both EU Member States and with other countries and to update privacy documentation/guidance .

## 2.0 Court of Justice of European Union (CJEU) preliminary ruling finds that Member State may unilaterally revoke Article 50 notice[[1]](#footnote-1)

2.1 The CJEU was asked for a preliminary ruling on the following question:

*‘Where, in accordance with Article 50 TEU, a Member State has notified the European Council of its intention to withdraw from the European Union, does EU law permit that notice to be revoked unilaterally by the notifying Member State; and, if so, subject to what conditions and with what effect relative to the Member State remaining within the European Union?’*

2.2 Both the UK Government and the lawyers for the European Council and Commission argued against the proposition of unilateral revocation of notice of withdrawal on different grounds.

2.3 The UK Government took the positon that the reference to the CJEU ought to be ruled inadmissible as it raised a hypothetical issue given that the policy of the UK Government is not to revoke Article 50.

2.4 The lawyers for the European Council and the Commission though willing to accept that notice could be revoked argued that Member States should not have the right to unilaterally withdraw their intention to leave on the basis that:

* any right of unilateral revocation could be used as leverage in negotiations, opening the way for abuse by the Member State concerned to the detriment of the European Union and its institutions;
* enabling for example the Member State to revoke its intention to leave shortly before the end of the period laid down in Article 50(3) TEU allowing it to then notify a new intention to withdraw immediately after that period expired triggering a new two-year negotiation period and rendering the timetable laid down in Article 50(3) TEU ineffective.

2.5 The CJEU dismissed the arguments of both the UK Government and European Council and the Commission:

* as the reference initiated by Members of the United Kingdom Parliament sought an interpretation of EU law and they had a legitimate interest in doing so as the answer on that question of law clarifies the options open to them in exercising their parliamentary mandates;
* withdrawing from a treaty was "by definition a unilateral act";
* the wording of Article 50(2) requires Member States to notify the European Council of an "intention" to withdraw from the EU, rather than taking a (binding) decision to do so;
* Article 50 enshrines the sovereign right of a Member State to withdraw from the European Union in accordance with its own constitutional requirements which is not a decision made in concert with the other Member States and therefore depends solely on the sovereign choice of the Member State;
* it would be contrary to the values of the EU and Article 50 to force a Member State that had decided not to withdraw to continue to negotiate a withdrawal agreement and to withdraw from the EU.

2.6 The CJEU ruled that Article 50 TEU must be interpreted as meaning that, where a Member State has notified the European Council, in accordance with that article, of its intention to withdraw from the EU, that article allows that Member State:

* for as long as a withdrawal agreement concluded between that Member State and the European Union has not entered into force or, if no such agreement has been concluded, for as long as the two-year period laid down in Article 50(3) TEU, possibly extended in accordance with that paragraph, has not expired;
* to revoke that notification unilaterally, in an unequivocal and unconditional manner, by a notice addressed to the European Council in writing, after the Member State concerned has taken the revocation decision in accordance with its constitutional requirements;.
* to maintain continued EU membership under terms that are unchanged as regards its status as a Member State, and to bring the withdrawal procedure to an end.

**3.0 Data Protection & Brexit**

3.1 If an agreement between the United Kingdom and the European Union (EU) is not approved by Parliament, and nothing further occurs, the UK shall cease to be a Member State and will automatically leave the European Union on 29th March 2019.

3.2 The manner of the UK’s departure from the EU has implications for the ease with which personal data continues to flow after that date between the UK and EU (including the European Economic Area (EEA)).

3.3 The UK Government’s stated data protection objective has been to reach an agreement with the EU whereby:

* each side mutually recognises the equivalence of their respective data protection regimes;
* provides a continuing role for the UK’s Information Commissioner:
	+ as a competent supervisory authority for the purposes of GDPR, and
	+ maintains its seat on the European Data Protection Board (EDPB).

3.4 The proposed UK model[[2]](#footnote-2) has so far been dismissed by the EU negotiators on the basis that:

* the UK refuses (at least in the longer term) to be subject to the jurisdiction of the Court of Justice of the European Union (CJEU) which settles disputes over the interpretation of the GDPR;
* the EU has no authority to ensure that the UK keeps pace with EU data protection standards as the GDPR is amended and supplemented over time.

3.5 In any case, Article 45 of the GDPR sets out the rules to be followed by the EC Commission in determining whether a third country or international organisation applies an adequate level of data protection.

3.6 The EU’s position is that this process cannot commence until the UK leaves the EU and becomes a third country.

3.7 Although there are other options open to Parliament, for the purposes of assessing the data protection implications of Brexit, this report focuses only on the UK:

* leaving the EU on the basis of an agreed Withdrawal Agreement;
* leaving the EU without a deal.

**4.0 Leaving the EU on basis of an agreed deal**

4.1 Once the UK leaves the EU, the GDPR no longer has direct effect in the UK.

4.2 However, section 3 of the European Union (Withdrawal) Act 2018 makes provision for the implementation of all direct EU legislation, including the GDPR, into national law.

4.3 This allows for decisions to be made (when time permits) as to the legislative changes needed once operating solely in a UK jurisdictional context.

4.4 The draft Withdrawal Agreement negotiated by the UK Government and the EU which Parliament is to vote on before 21st January 2019, includes provision for a two year transition period.

4.5 For the duration of that period, it is generally acknowledged that this would mean:

* EU laws (including the jurisdiction of the CJEU) continue to apply to the UK;
* the UK is treated in most respects as if it remains as a Member State for the purposes of EU laws, including the GDPR.

4.6 On this basis, the intention is that the UK would not be treated as a ‘third country’ for data transfer purposes until at least 1st January 2021 and that personal data would continue to flow without interruption, as now, without the need for any additional safeguards and/or documentation.

4.7 The assumption is that during such a transitional period, progress will be made in securing both an ‘adequacy’ decision and a long term trading relationship between the UK and the EU which once concluded would bring the Withdrawal Agreement to an end.

**5.0 Leaving the EU without a deal**

5.1 In the event the UK leaves the EU without a deal on 29th March 2019, there will be no transitional 2 year period.

5.2 As a consequence considerable clarifying amendments would be urgently needed to the GDPR removing references to EU Member States, Union law and the European Commission so that the wording continued to make sense once the UK becomes a ‘third country’.

5.3 The Government has recognised the importance of this and in mid-December announced its intention to publish draft amending legislation (see Section 7).

5.4 Where data transfers involve third countries and no adequacy agreement applies, Article 46 of the EU GDPR provides for data transfers subject to appropriate safeguards (other than in specific mainly one off situations warranting an exception).

.

5.5 Article 46(2) sets out the appropriate safeguards that must be in place for data transfers without the need for specific authorisation from a relevant supervisory authority.

5.6 These are:

* a legally binding and enforceable instrument between public authorities or bodies;
* binding corporate rules in accordance with Article 47;
* standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
* standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
* an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including data subjects’ rights[[3]](#footnote-3); or
* an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including data subjects’ rights[[4]](#footnote-4).

5.7 Alternatively, Article 46(3) provides that with direct authorisation from the competent supervisory authority, appropriate safeguards may be provided for in:

* contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
* for provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

5.8 Under either of the above models, it is evident that UK businesses involved in complex processing activities across multiple Member States and their EU partners will expend considerably more time, expense and administration managing the above data transfer requirements in comparison to the free flow of personal data that now applies across all Member States.

5.9 Moreover, it is also important to note that even though the UK legislative framework is closely aligned with EU data protection standards, once the UK leaves the EU and becomes a third country:

* the derogations and exemptions the GDPR permits Member States to make (and which the UK has created in the DPA 2018), will no longer be recognised under EU data protection law once the UK ceases to be a Member State;
* this means that when considering the legal basis for EU processing/transfers involving UK organisations, the applicable conditions will be limited to those in the GDPR as supplemented by particular EU Member States *(e.g. excluding those added by the UK under Schedules 1 and 2 of the DPA 2018);*
* UK based organisations:
	+ such as controllers or processors not established in the EU but engaging in processing activities falling within Article 3(2) (e.g. offering goods or services / monitoring the behaviour of EU citizens) may be required to appoint a representative located in an EU/EEA state to act for the organisation on EU GDPR compliance (unless an exception applies[[5]](#footnote-5));
	+ may benefit from a single lead data protection supervisory authority regulating processing activities across multiple EU Member States under the One Stop mechanism but if also processing UK citizen data, will be subject to UK data protection regulation and enforcement by the ICO;
	+ may need more than a UK based DPO to satisfy ‘accessibility’ requirements *(though the ICO’s* [*‘Six Steps to Take’*](https://ico.org.uk/media/for-organisations/documents/2553958/leaving-the-eu-six-steps-to-take.pdf) *guide states that if a DPO is in place they can continue in the same role for both the UK and EU)*

5.10 These are the minimum considerations that organisations selling into EU markets and/or involved in regular EU data transfers will need to speedily consider in the event of a ‘no deal’ scenario arising at the end of March.

5.11 However, ICO guidance indicates that after Exit Day organisations will need to consider two sets of rules[[6]](#footnote-6):

* **UK data protection rules**: if making a restricted transfer outwards from the UK; and
* **Other non UK data protection rules:** if receiving personal data from outside the UK (including from the EEA) into the UK.

5.12 This is because additional regulatory requirements will flow from the Government’s recently published draft instrument seeking to amend UK data protection law.

5.13 As further explained in section 7, this draft statutory instrument intends to create a mirror image of the GDPR in UK law – to be known as the ‘UK GDPR’ – with all the same features on extra-territorial scope and rules for controllers and processors processing UK data outside the UK as those that exist under the international data transfer rules in relation to ‘third countries’ under the (EU) GDPR, referenced earlier.

**6.0 DCMS statement on amendments to data protection law if UK leaves EU without a deal**

6.1 Following on from its earlier statement in September[[7]](#footnote-7), the DCMS issued a further notice on 13th December 2018 outlining the need for and substance of a draft instrument amending data protection law if the UK leaves the EU without a deal[[8]](#footnote-8).

6.2 The notice explains that appropriate changes are being made to the GDPR and the Data Protection Act 2018:

* to ensure the UK data protection framework continues to operate effectively after the UK ceases to be an EU Member State, and
* that the regulations and more detailed guidance are to be published in the next few weeks.

## 7.0 Draft Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019[[9]](#footnote-9)

7.1 The draft Regulations have now been published and laid before Parliament.

7.2 The Regulations seek to:

* Preserve EU GDPR standards in UK domestic law by creating a single regime for general processing to be known as the “UK GDPR” achieved by:
	+ removal of references to EU Member States, institutions, procedures and decision-making processes that will no longer be relevant after Exit Day, and
	+ replacement, where appropriate, with references that will operate correctly in domestic law;
	+ merging the EU GDPR as rewritten for the UK context with the “applied GDPR” (introduced in the UK DPA 2018 to extend the EU GDPR standards to certain processing activities outside the scope of EU law, such as the interface between privacy rights and public access information legislation);
	+ assigning functions residing with the European Commission under the EU GDPR to the Secretary of State or the Information Commissioner under the proposed UK GDPR.
* Amend the DPA 2018 and retain separate regimes for law enforcement and intelligence services processing;
* Preserve the effect of adequacy decisions made directly by the EU Commission in respect of a country or territory outside of the EU prior to Exit Day by writing these into the UK GDPR on a transitional basis;
* Transitionally recognises all EEA countries (including EU Member States) and Gibraltar as ‘adequate’ allowing data flows from the UK to the EU to continue;
* Introduce a modified version of the EU-US Privacy Shield for the UK;
* Deal with the international transfer of personal data by introducing powers for the Secretary of State to make “adequacy regulations”;
* Preserve the extra-territorial applicability of the EU GDPR in the UK GDPR to cover controllers and processors outside the UK (both within and outside the EEA), in certain circumstances;
* Oblige non-UK controllers who are subject to the UK data protection framework to appoint representatives in the UK if they are processing UK data on a large scale;
* Recognise EU Standard Contractual Clauses (SCCs) in UK law and give the ICO the power to issue new clauses[[10]](#footnote-10)
* Recognise Binding Corporate Rules (BCRs) authorised before Exit Day; and provide for the Information Commissioner to continue to approve Binding Corporate Rules (for the relatively small number of companies these rules apply to);
1. Amend the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2003/2426*) (PECR) to add the EU GDPR definition of consent.

7.3 These regulations are being made under:

* powers in the European Union (Withdrawal) Act 2018 (EUWA). (Section 8 of EUWA enables a minister to make regulations to correct deficiencies in retained EU law arising from withdrawal, such as a failure to operate effectively);
* section 211(2) of the Data Protection Act 2018 (DPA 2018) (in relation to consequential amendments to other legislation), and
* section 2(2) of the European Communities Act 1972 to amend the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

7.4 This amending legislation and many other similar statutory instruments are intended to come into effect in the event of a ‘no-deal’ scenario on Exit Day (29th March 2019).

7.5 But if there is a deal, most EU law will continue to apply in the UK during the transition period.

7.6 In that case legislative measures would be needed to cancel or delay implementation of this and other instruments (if already passed) until after the end of the transition period.

7.7 In either case (deal or no deal), the provisions amending the PECR (adding the EU GDPR definition on consent) are intended to come into force on 29 March 2019.

7.8 This statutory instrument will be subject to the affirmative resolution procedure.

**8.0 ICO advice on Data Protection and Brexit[[11]](#footnote-11)**

8.1 Coinciding with the notice issued by DCMS, the ICO has published guidance on the implications of ’no deal’ in the context of existing personal data flows between organisations in the UK and the EU and reliance on existing EU adequacy agreements.

8.2 This is primarily aimed at organisations, especially in the commercial sector and does not touch on cross border policing and security.

8.3 The guidance includes practical advice to help organisations plan ahead, comprising:

* a [‘Six Steps to Take’](https://ico.org.uk/media/for-organisations/documents/2553958/leaving-the-eu-six-steps-to-take.pdf) guide[[12]](#footnote-12);
* broader [guidance on the effects of leaving the EU without a withdrawal agreement[[13]](#footnote-13),](https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-there-s-no-brexit-deal/) which is of relevance to organisations:
	+ operating in the EEA, which includes the EU; or
	+ sending personal data outside the UK; or
	+ receiving personal data from the EEA

and those subject to any of the following regulations:

* + the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR);
	+ the Network and Information Systems Regulations 2018 (NIS); or
	+ Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).
* a general overview in the form of Frequently Asked Questions[[14]](#footnote-14);
* an [interactive guide](https://ico.org.uk/for-organisations/data-protection-and-brexit/standard-contractual-clauses-for-transfers-from-the-eea-to-the-uk-interactive-tool/) mainly for businesses to determine whether Standard Contractual Clauses are needed between themselves and organisations outside the UK[[15]](#footnote-15) (e.g. EEA states and other non EEA jurisdictions);
* templates containing the last approved (pre GDPR) [EU Commission templates with Standard Contractual Clauses (SCCs) for ‘controller to controller’ and controller to data processor’](https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-there-s-no-brexit-deal/the-gdpr/international-data-transfers/)[[16]](#footnote-16)

8.4 Within the ICO’s Six Steps Guide, organisations are encouraged to identify existing regular data flows/transfers involving the EU and other countries.

8.5 Although the UK Government intends to permit the free flow of data from the UK to the EU after Brexit, it cannot compel EU Member States.to do the same.

8.6 Whilst this is likely to impact the commercial sector most and it is unlikely that Councils are involved in processing data relating to EU citizens or monitoring their behaviour, if councils use cloud based processors with physical servers located in the EU this could prompt requests for contractual modifications/variations from EU based data processors.

8.7 After the Exit Day, data transfers from the UK to non EU countries, including those now covered by the EU adequacy agreements (including the EU/US Privacy Shield[[17]](#footnote-17)), will be subject to new UK GDPR data transfer and documentation requirements.

8.8 The ICO therefore recommends that in preparing for the possibility of ‘no deal’ organisations urgently identify (via information audits) what if any personal information is now regularly:

* **sent outside the UK; or**
* **received from the EEA; or**
* **received from countries or territories which are now covered by an EU adequacy decision**

**9.0 Conclusion**

9.1 Once the UK leaves the EU, consequential changes will need to be made to the EU derived GDPR. These will either be implemented at the end of March or whenever any transitional period ends.

9.2 This will clearly impact business and the commercial sector more than local authorities.

9.3 The timing and speed of any changes will depend on decisions yet to be made by Parliament in the next week or so.

9.4 If the UK leaves the EU by the end of March 2019, as a minimum local Councils will need to:

* review regular data flows and transfers from/to the EEA and other countries in preparation for implementing additional transfer documentary requirements necessary to satisfy EU or UK GDPR laws;
* review internal communications (and internal guidance and training materials) to ensure that those who need to know are made aware of the changes to UK data protection law and the reasons for this;
* external privacy notices and documentation to ensure these are consistent with updated UK law on data protection post Brexit;
* reference/definitions to data protection legislation in contractual and commercial agreements to ensure these are correct;

9.5 A further report will be made once the position is clearer and if new legislation is imminent, this will contain a detailed analysis of the differences/similarities between the current GDPR and proposed UK GDPR.

1. Wightman and Others (Notification by a Member State of its intention to withdraw from the European Union - Judgment) [2018] EUECJ C-621/18 (10 December 2018)
[*http://www.bailii.org/eu/cases/EUECJ/2018/C62118.html*](http://www.bailii.org/eu/cases/EUECJ/2018/C62118.html)

UK Commons briefing paper on CJEU decision

<https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-8461> [↑](#footnote-ref-1)
2. HM Government: Technical Note: Benefits of a new data protection agreement (7th June 2018) https://www.gov.uk/government/publications/technical-note-on-data-protection [↑](#footnote-ref-2)
3. Approved Codes of Conduct not yet in use – mechanisms to be established [↑](#footnote-ref-3)
4. Approved certification mechanisms not yet in use – to be established [↑](#footnote-ref-4)
5. Exceptions: where processing is only ‘occasional’ or if a public authority [↑](#footnote-ref-5)
6. ICO: Guidance on the effects of leaving the EU without a withdrawal agreement: International transfers

<https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-there-s-no-brexit-deal/the-gdpr/international-data-transfers/> [↑](#footnote-ref-6)
7. DCMS: Data protection if there’s no Brexit deal (13th September 2018) <https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal> [↑](#footnote-ref-7)
8. DCMS: Amendments to UK data protection law in the event the UK leaves the EU without a deal on 29 March 2019 (13th December 2018) <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> [↑](#footnote-ref-8)
9. The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019<http://www.legislation.gov.uk/ukdsi/2019/9780111177594/contents> [↑](#footnote-ref-9)
10. The ICO has published the last approved EU Standard Contractual clauses in template format for ‘controller to controller’ and ‘controller to processor’

(Under heading “appropriate safeguards’) <https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-there-s-no-brexit-deal/the-gdpr/international-data-transfers/> [↑](#footnote-ref-10)
11. ICO blog on protection and Brexit: <https://ico.org.uk/about-the-ico/news-and-events/blog-data-protection-and-brexit-ico-advice-for-organisations/> [↑](#footnote-ref-11)
12. ICO: “Leaving the EU – 6 steps to take” <https://ico.org.uk/media/2553958/leaving-the-eu-six-steps-to-take.pdf> [↑](#footnote-ref-12)
13. ICO: Guidance on the effects of leaving the EU without a withdrawal agreement

<https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-there-s-no-brexit-deal/> [↑](#footnote-ref-13)
14. ICO: Frequently Asked Questions on Information rights and Brexit

<https://ico.org.uk/for-organisations/data-protection-and-brexit/information-rights-and-brexit-frequently-asked-questions/> [↑](#footnote-ref-14)
15. ICO: Interactive tool <https://ico.org.uk/for-organisations/data-protection-and-brexit/standard-contractual-clauses-for-transfers-from-the-eea-to-the-uk-interactive-tool/> [↑](#footnote-ref-15)
16. ICO: Guidance on the effects of leaving the EU without a withdrawal agreement: International data transfers – appropriate safeguards

 <https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-there-s-no-brexit-deal/the-gdpr/international-data-transfers/> [↑](#footnote-ref-16)
17. **ICO Guidance: EU/US Privacy Shield**

The UK government is making arrangements for its continued application to restricted transfers from the UK to the USA and there is further information on the US government’s [Privacy Shield website](https://www.privacyshield.gov/article?id=Privacy-Shield-and-the-UK-FAQs). If the UK exits the EU without the Withdrawal Agreement (‘No Deal’), UK businesses will continue to be able to transfer personal data to US organisations participating in the Privacy Shield provided those US organisations have updated their public commitment to comply with the Privacy Shield to expressly state that those commitments apply to transfers of personal data from the UK.

UK organisations wishing to continue to make transfers to US organisations under the Privacy Shield if the UK exits the EU without a deal will need to check that the US organisation has made the necessary update to its commitment to compliance with the Privacy Shield. Confirmation of the update should usually be possible simply by checking the US organisation’s publicly available privacy policy.

<https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-there-s-no-brexit-deal/the-gdpr/international-data-transfers/> [↑](#footnote-ref-17)