EUROPEAN DATA PROTECTION SUPERVISOR

Information note on international data transfers after Brexit

16 July 2019

1. Background information

According to the current state of play, the UK including Northern Ireland will leave the EU on 1 November 2019 at 00.00 am CET and will become a third country[1].

In case the EU and the UK sign the withdrawal agreement (Title VII), as negotiated by the end of 2018, before 1 November 2019, the data flows to the UK will not be immediately affected. The withdrawal agreement provides for the application of EU data protection law until 31 December 2020, and this period may be extended for another two years. The General Data Protection Regulation (GDPR), the law enforcement Directive (EU) 2016/680, the ePrivacy Directive and any other provisions governing the protection of personal data are considered as Union data protection law.

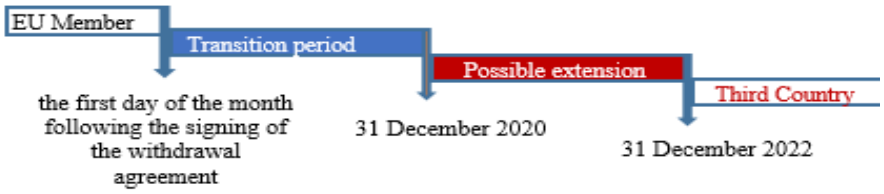


Fig. 1 Timeline foreseen in the Withdrawal Agreement

However, a no-deal Brexit scenario would have repercussions for the protection of personal data. This is because the EU primary and secondary law, including the data protection law, will cease to apply in the UK. Personal data transfers to the UK will be subject to specific conditions with which Union institutions and bodies (EUIs) need to comply. Some institutions and bodies are already familiar with the available data transfer mechanisms, as they are already transferring data to third countries outside the EEA.

Fig. 2 Timeline in case of a no-deal Brexit

The EDPS builds upon the guidance provided on this matter by the European Commission and by the European Data Protection Board.

[1] On the 7 May 2019, the UK government confirmed that it will hold European Parliament elections and therefore the UK will not leave the EU on 1 June 2019.

2. Data transfers from Union institutions and bodies to the UK in case of no-deal Brexit

In case of a no-deal Brexit the flow of data from EUIs to the UK and Northern Ireland will be subject to the requirements for international data transfers as laid down in Chapter V of Regulation (EU) 2018/1725 (EU DPR). For example, if an EUI outsources mission trips management or IT services to a processor in the UK, legal safeguards will be required for the personal data transferred to the UK.

2.1. International data transfers mechanisms

The EU DPR provides that a data transfer to a third country, such as the UK, shall not undermine the level of protection guaranteed by this Regulation (Article 46). This level of protection shall be maintained for onward transfers, i.e. transfers from the third country, such as the UK, to another third country or international organisation. For this purpose, the EU DPR lays down a series of mechanisms which the controllers and processors may choose to enable the transfer to a third country. It is up to them to assess which of the available mechanisms best reflects their situation.

2.1.1 Adequacy decisions

A transfer of personal data to a third country can take place when the European Commission has recognized this third country as offering an adequate level of protection (Article 47). The effect of such an adequacy decision is that personal data can flow from the EUIs to that third country as if the transfer takes place within the EU/EEA.
However, no such recognition of the UK legal framework will be in place before the UK leaves the EU and relevant negotiations will require time.
Therefore, EUIs shall consider adopting other transfer mechanisms from the ones provided in Chapter V.

2.1.2 Appropriate safeguards

There are a series of data transfer mechanisms adducing appropriate safeguards. Article 48 EU DPR lists all ‘appropriate safeguards’. A common feature of all is the condition that they must provide for enforceable and effective data subjects rights.

a. Instruments exclusively available to public authorities

EUIs as public authorities may consider to use the mechanisms which the EU DPR considers more apt to their situation (Article 48(2)(a) and (3)(b)).
One option is to use a legally binding and enforceable instrument, such as an administrative agreement, a bilateral or multilateral international agreement. The agreement must be binding and enforceable for the signatories.
The second option is to use administrative arrangements, such as Memoranda of Understanding. Although not legally binding themselves, they shall however provide for enforceable and effective data subject rights. The non-binding administrative arrangements are subject to an authorisation by the EDPS.

b. Standard Data Protection Clauses

In case EUIs are interacting with private entities (for instance, outsourcing mission trips management, IT services or training)[2], they may consider signing standard data protection clauses adopted by the European Commission. These contracts offer the additional adequate safeguards with respect to data protection that are needed in case of a transfer of personal data to any third country.
Three sets of standard data protection clauses are currently available (remaining valid under the GDPR until amended, replaced or repealed by a Commission decision):

- EU controller to third country (non EU/EEA) controller (e.g. UK): 2 Sets are available:
  - 2001/497/EC
  - 2004/915/EC
- EU controller to third country (non EU/EEA) processor (e.g. UK):
  - 2010/87/EC

It is important to note that the standard data protection clauses may not be modified and must be signed as provided. However, these contracts may be included in a wider contract and additional clauses might be added provided that they do not contradict, directly or indirectly, the standard data protection clauses adopted by the European Commission[3].
Any further modifications to the standard data protection clauses will imply that this will be considered as ad-hoc contractual clauses which will require a prior authorisation by the EDPS (analysed under e).
Finally, the EU DPR provides for the possibility of standard data protection clauses adopted by the EDPS and approved by the Commission. So far such clauses have not been adopted.

c. Binding Corporate Rules

Binding Corporate Rules are personal data protection policies adhered to by a group of undertakings (ie. multinationals) in order to provide appropriate safeguards for transfers of personal data within the group, including outside of the EU/EEA.
In case the processor of a specific activity is not an EUI, he may already make use of BCRs for processors (these binding corporate rules apply to data received from a controller established in the EU, which is not a member of the group, and then processed by the concerned group members as processors and/or sub-processors)[4]. BCRs authorised under the former Directive 95/46/EC remain valid under the GDPR (Article 46(5)) and are considered as a transfer mechanism adducing adequate safeguards according to the EU DPR (Art. 48(2)(d)). However, they need to be updated in order to be fully in line with the GDPR provisions.
Future Binding Corporate Rules must be approved by the competent national supervisory authority, following an opinion of the EDPB (Article 47(1) and 64(3) GDPR), prior to any transfer.

d. Codes of conduct and certification mechanisms

[2] EDPS, The transfer of personal data to third countries and international organisations by EU institutions and bodies, Position Paper, p. 20-22.
[3] See the following communication of the European Commission http://europa.eu/rapid/press-release_MEMO-05-3_en.htm.
[4] Article 29 Data Protection Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev. 1, 28 November 2017, available on the EDPB website.

In the event that the processor is not an EUI, codes of conduct or certification mechanisms, as provided in GDPR, can be used in order to offer appropriate safeguards for transfers to a third country.
These tools are new under GDPR and therefore the work of the EDPB, which is currently working on guidelines in order to further clarify the content and the use these tools, should be closely followed.

e. Ad hoc contractual clauses

In case EUIs are interacting with private entities, they can also make use of ad-hoc contractual clauses they negotiate with UK counterparts in order to provide appropriate safeguards taking into account their particular situation.
Prior to any transfer, these tailored contractual clauses must be authorised by the EDPS (Art. 48(3)(a) EU DPR).

2.1.3 Derogations [5]

In the absence of an adequacy decision, EUIs should first consider providing adequate safeguards, framing the transfer of personal data with one of the mechanisms mentioned under 2.1.2.

Derogations provided in Article 50 EU DPR are exemptions from the general principle that personal data may only be transferred to third countries if an adequate level of protection is provided for in the third country or if appropriate safeguards have been adduced and the data subjects enjoy enforceable and effective rights. Furthermore, transfers based on a derogation are not required to have any kind of prior authorisation from the EDPS, leading to increased risks for the rights and freedoms of the data subjects concerned. Therefore, derogations must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive.

Derogations are exhaustively mentioned in Article 50(1) EU DPR and include data transfers:

- where an individual has explicitly consented to the proposed transfer after having been provided with all necessary information about the risks associated with the transfer;
- where the data transfer is necessary for the performance of a contract to which a data subject is a part or for the implementation of pre-contractual measures;
- where the data 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;
- where the data transfer is necessary for important reasons of public interest;
- where the data transfer is necessary for the establishment, exercise or defence of legal claims;
- where the data transfer is necessary for the protection of the vital interests of the data subject or of other persons and the data subject is physically or legally incapable of giving consent and

[5] See also EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, regarding the similar provisions of the General Data Protection Regulation (GDPR).

- where a transfer is made from a public register.

3. Data transferred before the withdrawal date

The European Commission in the Position Paper on the Use of Data and Protection of Information Obtained or Processed before the withdrawal date concludes that UK based controllers and processors may continue to process personal data transferred before the withdrawal date only if these data enjoy the protection of EU data protection law. Such protection will be guaranteed, in case that a Withdrawal Agreement is put in place.

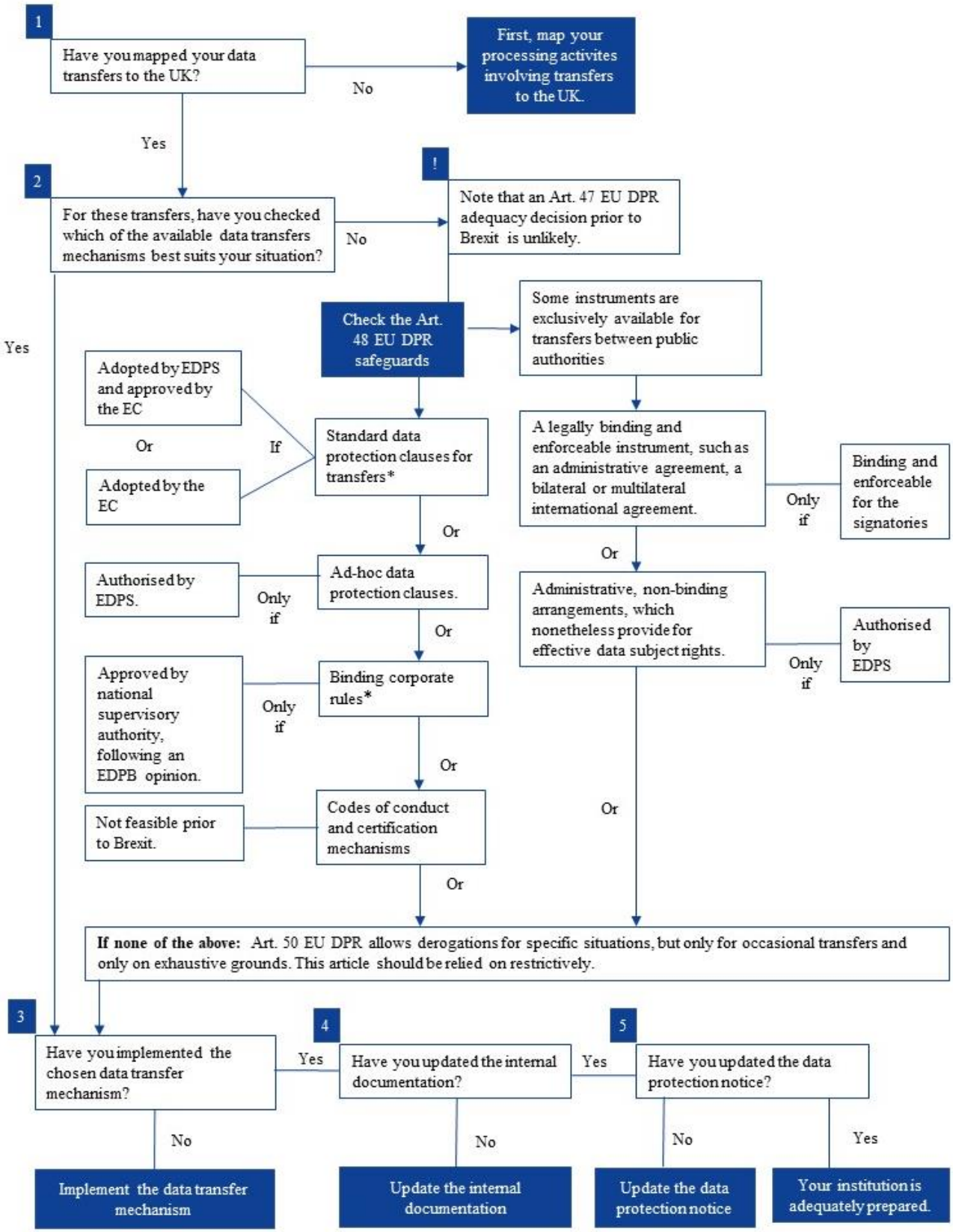
The developments on this sensitive issue should be closely followed and the EDPS may provide further guidance if is deemed necessary.

4. Steps to take in order to be prepared

In order to be prepared for the case of no-deal Brexit, EUIs should take the following steps:

i. map their processing activities;
ii. check the available data transfers mechanism that best suits their situation;
iii. implement the chosen data transfer mechanism before 1 June or 1 November 2019;
iv. update their internal documentation;
v. update their data protection notice accordingly.

4.1. In brief: steps to take in order to be prepared for a no-deal Brexit



* Binding corporate rules and standard contractual clauses (adopted by the EC) under the old Directive 95/46 are still valid, but will need to be updated over time in line with the GDPR. In any case, before using old EC standard contractual clauses you should make sure to adapt them to Regulation (EU) 2018/1725 [EU DPR].