Barry McManus

BREXIT, GDPR AND DATA TRANSFER FROM THE EU TO THE UK

DEFINITIONS

BREXIT: "British exit" the withdrawal of the United Kingdom (UK) from the European Union (EU).

DPA: UK Data Protection Act 2018.

ECJ: European Court of Justice, the supreme court of the European Union in matters of European Union law.

GDPR: General Data Protection Regulation.

ICO: The Information Commissioner Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

SCC: Standard Contractual Clause: safeguards for data protection and enforceable data subject rights and effective legal remedies for data subjects. (GDPR Article 46).

Schrems II: ECJ Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (called "Schrems II case") invalidated the EU-US Privacy Shield.

How to facilitate EU data transfer to a non-EU country

To recap from QUASAR #153, GDPR is concerned with the secure processing of PII outside of the EU. There are four avenues for this to occur(3):

1. 3rd Country Adequacy: PII can be processed within countries that are recognised by the EU to have an adequate level of data protection, such as New Zealand, Switzerland and Uruguay (6). The UK are undergoing an adequacy decision.
2. Specific treaty: For the US, secure processing of PII could not be ascertained and the EU-US Privacy Shield treaty was established to ensure data privacy and security. This treaty was the focus of the ECJ ruling.
3. Individual Contract: A business transferring PII puts in place certain safeguards to ensure protection via a contract, such as: the subject-matter and duration of the processing. This may be an individual contract or Standard Contractual Clauses (SCCs) (3) which are adopted by the commission or by a supervisory authority.
4. Inter organisation transfer: Binding Corporate Rules (BCRs), similar to contracts, are corporate policies enforced by every sub member of a multi country organisation.

ADEQUACY DETERMINATION

EU countries are required to bring GDPR into their own legal system(4) and have passed or will pass their own data protection bills. The UK government brought EU GDPR into UK law via the Data Protection Act (DPA) 2018(5) .

Now that the UK has left the EU, the EU is reviewing UK law to establish if the DPA aligns with GDPR. This review is termed the "adequacy decision". In order for the EU to make a judgement, it has applied a four-month delay on data transfer restrictions (to the end of April 2021). This may be extended until the end of June. During the EU review period, there is no restriction of the transfer of data from the EU to the UK. The UK government has stated that it will not restrict the transfer of data from the UK into the EU.

If 3rd country adequacy is determined, then the DPA fulfils the needs of GDPR. The UK will be able to transfer data from the EU to the UK as if it had never left the EU.

Should the EU determine that there is divergence within UK law, then it is bound to implement data transfer restrictions on the UK. The EU will treat the UK in the same manner as, for example, the USA. If an organisation decides to transfer data to the UK, then it will need to ensure that adequate controls exist to protect data.

Given that the DPA is the incorporation of the EU GDPR law then it should be expected that this "adequacy" decision is granted.

However, this may not be as straight forward as it appears.

1) Any alignment divergence from EU GDPR may raise questions over compliance of data transfer to the UK.
2) Other UK laws may impact adequacy. QUASAR#153 discussed the impact of the Schrems II ruling concerning US intelligence agencies surveillance practices(6). The UK Investigatory Powers Act 2016 grants surveillance powers to British law enforcement to use PII. This act requires internet service providers and mobile telephony companies to maintain records on items such as internet browser activity and retain it for 12 months(7).

DATA PROTECTION IMPACT ASSESSMENT

There is a level of uncertainty around the outcome of the EU's adequacy decision which will impact UK companies. The UK Information Commissioner's Office (ICO) (8) recommends that UK organisations should consider implementing additional safeguards to ensure data protection. To do that they need to "know" the data:

- Perform a Data Impact Assessment: Both, GDPR and DPA state the need for an impact assessment to close out any gaps in data protection:
  - Identify the data being processed/held and the lawful basis for doing so.
  - Review the personal data and decide what is necessary for processing and what is optional. (Securely destroy anything that is not necessary).
  - State and record how long data will be retained. Ensure data is not retained for longer than necessary.
  - Regularly check that the data is still relevant and accurate.
  - Regularly review security arrangements.
  - Ensure staff are trained on how people can exercise their rights regarding the data being held.
  - Create a privacy notice for people to understand why their data is being held and why.
  - Perform a data impact assessment for sub processors.
- **Complying to UK Data Privacy Act 2018:** This is the current law. It is good practice to perform the data impact assessment(5) so that individual rights can be exercised (e.g., right to rectification as per UK Data Privacy(5), chapter 3, section 46).

It may be prudent to ascertain when data was collected. Any data collected prior to 01-Jan-21 is bound by GDPR , any data collected after 31-Dec-20 will be bound by UK Data Privacy Act rules, (8). The ICO states that it would be useful to know which rules pertain to which data set, especially should the UK GDPR rules diverge in the

future. Should an adequacy decision be made, then the UK rules will cover both datasets. But again, even if the UK Act is reflective of GDPR, the impact of other UK laws may mean that this is not guaranteed.

MITIGATIONS FOR NON-3RD COUNTRY ADEQUACY DECISION

To mitigate against not attaining 3rd country adequacy, the UK hoped to expedite treaty attainment by leveraging the US-EU privacy Shield as a specific treaty. Given Schrems II outcome, there will likely be a delay in the generation of a UK-EU treaty.

1) Generate Standard Contractual Clause

Use the Data Impact Assessment to facilitate Standard Contractual Clauses or Binding Corporate Rules will be the approach for organisations to take to ensure adequate protection safeguards required by the EU:

2) Seek a GDPR representative

Designate a representative in the EU/EEA to deal with EU and individuals on the organisation's behalf(3).

- Identify an individual or organisation (law firm, consultancy or other company) in a relevant EU state who provides services as a GDPR representative.
- Authorise them in writing to act on your behalf.
- Include their contact details in your privacy information.

3) Remember Policies and Standard Operating Procedures (SOPS)

Amend internal policies, SOPs etc to reflect any changes from the impact assessment or implementation of SSCs.

SUMMARY

The EU is undergoing an "adequacy decision" exercise to ascertain the compliance of UK Data Privacy Act 2018 to EU GDPR. The adequacy decisions are reviewed periodically, at least every 4 years (GDPR(3) Article 45, Clause 3).

The GDPR has been incorporated into the UK DPA and the ICO has stated that there is little change in the principles, rights and obligations within the DPA(5).

However, the ICO recommends that organisations that receive EU PII data after 30th April 2021 should put alternative safeguards in place(8). The author recommends performing a Data Protection Impact Assessment as a starting point and using its outcome to generate a SCC.

REFERENCES

1) Tech firms like Facebook must restrict data sent from EU to US, court rules, www.theguardian.com/technology/2020/jul/16/tech-firms-like-facebook-must-restrict-data-sent-from-eu-to-us-court-rules Guardian, 16 July 2020
2) The end of Privacy Shield spells trouble for Brexit Britain, https://www.wired.co.uk/article/privacy-shield-future Wired 17 July 2020
3) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
4) European Commission Adequacy Decisions, Recognised countries that offer adequate level of data protection, https://gdprinformer.com/gdpr-articles/data-transfers-third-countries
5) Example SCC: European Data Protection Board Website, January 2020 https://edpb.europa.eu/sites/edpb/files/files/file2/dk_sa_standard_contractual_clauses_january_2020_en.pdf
6) Source of example SCC: Register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism, European Data Protection Board website https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions
7) Paragraphs 108 and 134/135, Case C 311/18, JUDGMENT OF THE COURT (Grand Chamber), 16 July 2020, http://curia.europa.eu/juris/document/document jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=9791227

'There is a level of uncertainty around the outcome of the EU's adequacy decision which will impact UK companies.'

GDPR 3	UK DATA PRIVACY ACT(5)
Paragraph 81 indicates that "the activities performed by the processor should be governed by a contract". Gdpr paragraph 28.7 Indicates that the commission may lay down standard contractual clauses for the items listed in article 28.3 And article 28.4".	Section 59, (5) states "The processing by the processor must be governed by a contract in writing". The term Standard Contractual Clauses is not used within DPA.
GDPR Paragraph 28.3 states the processor: a. Processes on the documented instructions of the controller b. Is committed to confidentiality. c. Takes all measures detailed in Article 32 (Security of Processing, based on risk: data pseudonymisation and encryption; ensure confidentiality, integrity, availability and resilience of processing; restore access to data; regular assessment of technical and organisational measures for security of processing. d. Ensures due consideration for engaging another processor. e. Ensures data subject rights (right to be forgotten, correction, deletion, etc) . f. Notifies of data breach and data impact assessment (in the event of high risk to the data subject). g. Deletes or returns personal data at the end of processing. h. Provides information to demonstrate compliance. Paragraph 28.4 state that the same obligations shall be imposed on a sub processor when a processor engages a sub processor via a contract.	Section 59 (6) states that the processor must: a) act only on instructions from the controller, b) ensure that the persons authorised to process personal data are subject to .. confidentiality, c) assist the controller by any appropriate means to ensure compliance with the rights of the data subject under this Part, d) at the end of the provision of services by the processor to the controller— (i) either delete or return to the controller (at the choice of the controller) the personal data to which the services relate, and (ii) delete copies of the personal data unless subject to a legal obligation to store the copies, e) make available to the controller all information necessary to demonstrate compliance with this section, and f) comply with the requirements of this section for engaging sub-processors (e.g., security of processing, data breach notification, Data Impact Assessment…).