Post Brexit – An Update on the United Kingdom Privacy Regime

Post Brexit – An Update on the United Kingdom Privacy Regime

2021/9/10

After lengthy talks, on 31 January 2020, the United Kingdom ('UK') finally exited the European Union ('EU'). Then, the UK shifted into a transition period. The UK government was bombarded with questions from all stakeholders. In particular, the data and privacy industry yelled out the loudest – what am I going to do with data flowing from the EU to the UK? Privacy professionals queried – would the UK have a new privacy regime that significantly departs from the General Data Protection Regulation ('GDPR')?

Eventually, the UK made a compromise with all stakeholders – the British, the Europeans and the rest of the world – by bridging its privacy laws with the GDPR. On 28 June 2021, the UK obtained an adequacy decision from the EU.[1] This was widely anticipated but also widely known to be delayed, as it was heavily impacted by the aftermaths of the invalidation of the US- EU Privacy Shield.[2]

While the rest of the world seems to silently observe the transition undertaken by the UK, post-Brexit changes to the UK's privacy regime is not only a domestic or regional matter, it is an international matter. Global supply chains and cross border data flows will be affected, shuffling the global economy into a new order. Therefore, it is crucial as citizens of a digital economy to unpack and understand the current UK privacy regime.

This paper intends to give the reader a brief introduction to the current privacy regime of the UK. The author proposes to set out the structure of the UK privacy legislation, and to discuss important privacy topics. This paper only focuses on the general processing regime, which is the regime that is most relevant to general stakeholders.

UK Privacy Legislation

There are two main privacy legislation in the UK – the *Data Protection Act 2018* ('DPA') and the *United Kingdom General Data Protection Act* ('UK GDPR'). These two acts must be read together in order to form a coherent understanding of the current UK privacy regime.

The UK GDPR is the creature of Brexit. The UK government wanted a smooth transition out of the EU and acknowledged that they needed to preserve the GDPR in their domestic privacy regime to an extent that would allow them to secure an adequacy decision. The UK government also wanted to create less impact on private companies. Thus, the UK GDPR was born. Largely it aligns closely with the GDPR, supplemented by the DPA.

ICO

The Information Commissioner's Office ('ICO') is the independent authority supervising the compliance of privacy laws in the UK. Prior to Brexit, the ICO was the UK's supervisory authority under the GDPR. A unique feature of the ICO's powers and functions is that it adopts a notice system. The ICO has power to issue four types of notices: information notices, assessment notices, enforcement notices and penalty notices.[3] The information notice requires controllers or processors to provide information. The ICO must issue an assessment notice before conducting data protection audits. Enforcement is only exercisable by giving an enforcement notice. Administrative fines are only exercisable by giving a penalty notice.

Territorial Application

Section 207(1A) of the DPA states that the DPA applies to any controller or processor established in the UK, regardless where the processing of personal data takes place. Like the GDPR, the DPA and the UK GDPR have an extraterritorial reach to overseas controllers or processors. The DPA and the UK GDPR apply to overseas controllers or processors who process personal data relating to data subjects in the UK, and the processing activities are related to the offering of goods or services, or the monitoring of data subjects' behavior.[4]

Transfers of Personal Data to Third Countries

On 28 June 2021, the UK received an adequacy decision from the EU.[5] This means that until 27 June 2025, data can continue to flow freely between the UK and the European Economic Area ('EEA').

As for transferring personal data to third countries other than the EU, the UK has similar laws to the GDPR. Both the DPA and the UK GDPR restrict controllers or processors from transferring personal data to third countries. A transfer of personal data to a third country is

permitted if it is based on adequacy regulations.[6] An EU adequacy decision is known as 'adequacy regulations' under the UK regime.

If there is no adequacy regulations, then a transfer of personal data to a third country will only be permitted if it is covered by appropriate safeguards, including standard data protection clauses, binding corporate rules, codes of conduct, and certifications.[7] The ICO intends to publish UK standard data protection clauses in 2021.[8] In the meantime, the EU has published a new set of standard data protection clauses ('SCCs').[9] However, it must be noted that the EU SCCs are not accepted to be valid in the UK, and may only be used for reference purposes. It is also worth noting that the UK has approved three certification schemes to assist organizations in demonstrating compliance to data protection laws.[10]

Lawful Bases for Processing

Basically, the lawful bases for processing in the UK regime are the same as the GDPR. Six lawful bases are set out in article 6 of the UK GDPR. To process personal data, at least one of the following lawful bases must be satisfied:[11]

1. The data subject has given consent to the processing;
2. The processing is necessary for the performance of a contract;
3. The processing is necessary for compliance with a legal obligation;
4. The processing is necessary to protect vital interests of an individual – that is, protecting an individual's life;
5. The processing is necessary for the performance of a public task;
6. The processing is necessary for the purpose of legitimate interests, unless other interests or fundamental rights and freedoms override those legitimate interests.

Rights & Exemptions

The UK privacy regime, like the GDPR, gives data subjects certain rights. Most of the rights granted under the UK privacy regime is akin to the GDPR and can be found under the UK GDPR. Individual rights under the UK privacy regime is closely linked with its exemptions, this may be said to be a unique feature of the UK privacy regime which sets it apart from the GDPR. Under the DPA and the UK GDPR, there are certain exemptions, meaning organizations are exempted from certain obligations, most of them are associated with individual rights. For example, if data is processed for scientific or historical research purposes, or statistical purposes, organizations are exempted from provisions on the right of access, the right to rectification, the right to restrict processing and the right to object in certain circumstances.[12]

Penalties

The penalty for infringement of the UK GDPR is the amount specified in article 83 of the UK GDPR.[13] If an amount is not specified, the penalty is the standard maximum amount.[14] The standard maximum amount, at the time of writing, is £8,700,000 (around 10 million Euros) or 2% of the undertaking's total annual worldwide turnover in the preceding financial year.[15] In any other case, the standard maximum amount is £8,700,000 (around 10 million Euros).[16]

Conclusion

The UK privacy regime closely aligns with the GDPR. However it would be too simple of a statement to say that the UK privacy regime is almost identical to the GDPR. The ICO's unique enforcement powers exercised through a notice system is a distinct feature of the UK privacy regime. Recent legal trends show that the UK while trying to preserve its ties with the EU is gradually developing an independent privacy persona. The best example is that in regards to transfers to third countries, the UK has developed its first certification scheme and is attempting to develop its own standard data protection clauses. The UK's transition out of the EU has certainly been interesting; however, the UK's transformation from the EU is certainly awaited with awe.

[1] Commission Implementing Decision of 28.6.2021, *pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom*, C(2021) 4800 final, https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf..

[2] Judgment of 16 July 2020, *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems*, C-311/18, EU:C:2020:559, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311.

[3] *Data Protection Act 2018*, §115.

[4] *Data Protection Act 2018*, §207(1A); *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, art 3.

[5] *supra* note 1.

[6] *Data Protection Act 2018*, §17A-18; *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, art 44-50.

[7] *Data Protection Act 2018*, §17A-18; *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, art 46-47.

[8]International transfers after the UK exit from the EU Implementation Period, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/ (last visited Sep. 10, 2021).

[9] Standard contractual clauses for international transfers, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

(last visited Sep. 10, 2021).
[10] ICO, *New certification schemes will "raise the bar" of data protection in children's privacy, age assurance and asset disposal*, ICO, Aug. 19, 2021, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/08/ico-approves-the-first-uk-gdpr-certification-scheme-criteria/ (last visited Sep. 10, 2021).
[11] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art 6(1)-(2); Lawful basis for processing, ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ (last visited Sep. 10, 2021).
[12] *Data Protection Act 2018*, sch 2, part 6, para 27.
[13] *id.* at §157.
[14] *id.*
[15] *id.*
[16] *id.*

Links

- Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems
- International transfers after the UK exit from the EU Implementation Period
- Standard contractual clauses for international transfers
- New certification schemes will "raise the bar" of data protection in children's privacy, age assurance and asset disposal
- Lawful basis for processing

Download

- pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom [pdf]

Jasmine Chou
Associate Legal Researcher

Release : 2021/09