ELVINGER HOSS
LUXEMBOURG LAW

EACCNY "Brexit, What's Next?" Series | EU-UK Data Protection Law Divergence: Impact on Data flows

1. Post-Brexit UK regime

Following the end of the Brexit transition period, the United Kingdom has retained the General Data Protection Regulation (Regulation 2016/679) ("**EU GDPR**") as part of its national laws, as the "**UK GDPR**", under the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419) (as amended) ("**Regulations**").

The UK GDPR sits alongside the Data Protection Act 2018 ("**DPA**") and the Privacy and Electronic Communications Regulations ("**PECR**") as the backbone of the UK's post-Brexit data protection regime. The Regulations amended the UK GDPR, DPA and PECR to make them work properly as domestic law through relatively functional changes, under which the key substance of the EU GDPR remained. However, the UK now could diverge from EU data protection law through domestic statutory reform and the UK Government is considering steps in that direction.

2. Adequacy Decisions adopted

On 28 June 2021, just before the interim bridging mechanism enshrined in the EU-UK Trade and Cooperation Agreement expired on 30 June 2021, the European Commission ("**Commission**") adopted two adequacy decisions for the UK ("**Adequacy Decisions**"). The first decision concerned the EU **GDPR** and the second Law Enforcement Directive.

The adoption of the Adequacy Decisions, after months of negotiation, provided a degree of long-awaited legal certainty concerning the ongoing flow of personal data from the EU to the UK, including data exchanges in the law enforcement sector. Under this regime, businesses located in the EU can continue exporting personal data to the UK as current UK national laws have been recognised as offering a level of protection that is essentially equivalent to that under the EU GDPR.

The Adequacy Decisions are the first of their kind to have a sunset clause limiting their duration. The Adequacy Decisions expire four years from their entry into force, after

which they can be further extended. This sunset clause has been introduced to ensure that UK data protection law remains essentially equivalent to that of the EU while the UK is covered by adequacy decisions. This is a strong safeguard in case there is future divergence in UK data protection law away from the essentially equivalent level of protection which existed at the time of the assessment.

UK Consultation on Data Protection Reform

On 10 September 2021, the UK's Department for Digital, Culture, Media & Sport ("**DCMS**") released a consultation "**Data: A new direction**" (the "**Consultation**") with suggested reforms to the UK's data protection regime. The aim of the Consultation is to "create an ambitious, pro-growth and innovation-friendly data protection regime that underpins the trustworthy use of data". The Consultation's proposals represent significant divergence from the EU regime and trend towards a risk-based approach.

The key points are:

- **Accountability and governance.** Revoking existing obligations to perform data protection impact assessments, maintain records of processing, and appoint a data protection officer. These would be replaced by a privacy management program ("**PMP**"), which is intended to be a less rigid approach to accountability although the substance is relatively similar to the UK GDPR requirements. The proposed PMP demands clear responsibilities for compliance, policies and risk assessment tools and operational plans to monitor and revise the PMP.
- **Adequacy decisions.** Amending the framework for the UK's own adequacy decisions for data transfers, to be *"risk-based and focused on outcomes"* rather than a "*largely textual comparison of another country's legislation"* focussing on *"academic or immaterial"* risks. Adequacy decisions may also be included as a part of trade agreements with other countries. We observe the announcement from the DCMS that "*adequacy partnerships*" are already being progressed with many jurisdictions, including the US. That would represent a significant change from the EU approach, as the Commission is currently talking down prospects for an imminent replacement for the (now invalid) Privacy Shield transfer mechanism.
- **International Transfers.** Allowing organisations to create alternative transfer mechanisms, in addition to the standard form mechanisms already available under Article 46 of the UK GDPR. This may even look like a move back to the UK's pre-EU GDPR approach of allowing exporters to draft their own contractual transfer safeguards. This could benefit organisations with complex data transfer requirements for which the existing suite of mechanisms, such as the Standard Contractual Clauses, are not an effective way of safeguarding a data transfer.
- **Data breach reporting.** Stating that only data breaches that are likely to create a risk to the rights and freedoms of individuals **and** which are material would need to be reported to the Information Commissioner's Office ("**ICO**"). This would create different standards for reporting under the UK GDPR compared with the EU requirement, causing more complexities for organisations with a multi-national footprint.
- **DSAR's.** Reintroducing a nominal fee from the data subject for a data subject access request ("**DSAR**") along with the ability to impose a cost ceiling on a DSAR response and to refuse vexatious requests.
- **Legitimate interests.** Publishing a list of pre-approved legitimate interests, on which

an organisation could rely without the need to balance that interest against an individual's rights. Notably, the list includes audience measurement cookies for service users' devices, and the use of personal data for research and development to improve services.

Impact of Reform on Adequacy Decisions

On 13 April 2021, the EDPB adopted Opinion 14/2021 regarding the Commission's (then) draft adequacy decision of the UK under the EU GDPR.[1] At the time of providing that Opinion, the UK data protection framework was largely based on the EU data protection framework because the UK was a Member State of the EU up until 31 January 2020.

The EDPB nevertheless raised serious challenges and concerns to be monitored by the UK and the Commission, in particular: national security; intelligence and the surveillance regime of the UK (including access by public authorities to data transferred to the UK); and possible future divergence of the UK data protection framework. The resulting Adequacy Decisions follow a careful assessment by the Commission of UK law and practice with those challenges in mind. The conclusion of that assessment resides notably in the application of the DPA as amended to incorporate the principles of the EU GDPR into the UK GDPR, adhesion to the Council of Europe's Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (and Protocol 108+) and submission to the European Court of Human Rights.

Therefore, any amendment to the legal framework currently applicable in the UK and affecting its essentially equivalent level of data protection could put the Adequacy Decisions at risk. The Commission shall indeed, according to the Adequacy Decisions themselves, "*continuously monitor the application of the UK legal framework upon which the Adequacy Decisions are based, including the conditions under which onward transfers are carried out and individual rights are exercised*". In addition, EU "*Member States and the European Commission shall inform each other of [(a)] cases where the Information Commissioner, or any other competent United Kingdom authority, fails to ensure compliance with the legal framework upon which [the Adequacy Decisions are] based"* and of "*[(b)] any indications that interferences by United Kingdom public authorities with the right of individuals to the protection of their personal data go beyond what is strictly necessary, or that there is no effective legal protection against such interferences*".

Should the Commission become aware of indications that an adequate level of protection is no longer ensured, it can suspend, repeal or amend the Adequacy Decisions after informing the competent UK authorities. The Commission can also do the same in the event that adequacy can no longer be assessed due to any lack of cooperation of UK Government.

3. Key Questions for International Companies Present in the UK and EU

One-stop-shop and double jeopardy

Under the EU GDPR, an organisation engaged in cross-border processing may use the supervisory authority in the EU Member State where it has its main establishment as its lead supervisory authority ("**LSA**"). The benefit of this is that the LSA will be the sole interlocutor, or one-stop-shop ("**OSS**"), for that organisation. That mechanism no longer applies to the UK following the end of the Brexit transition period.

The UK GDPR applies to the processing of personal data by: (a) UK-established

businesses; and (b) controllers and processors established outside of the UK if their processing activities relate to offering goods or services to individuals in the UK or monitoring the behaviour of individuals taking place in the UK.

The EU GDPR in turn applies to the processing of personal data by: (a) EU-established businesses; and (b) controllers and processors established outside of the EU but offering goods or services to individuals in the EU or monitoring the behaviour of individuals taking place in the EU.

As a result, the two regimes may apply concurrently to the same processing activities by either UK-based businesses active in the EU or EU-based businesses active in the UK. Therefore, both UK-based and EU-based controllers and processors may fall within the scope of the supervision of the ICO and one or several supervisory authorities in the European Economic Area ("**EEA**"), with or without application of the OSS mechanisms. They may even face the "double jeopardy" of fines or other enforcement action being taken under both the EU GDPR and the UK GDPR. This will depend on whether or not any processing can be considered as cross-border and whether or not it is likely to substantially affect individuals in EEA states other than the one where the controller or processor is established.

One transfer, two regimes

A similar conclusion applies to transfers from the UK or the EEA to countries outside of the EEA as these transfers might fall within the scope of the UK GDPR (regarding personal data collected in the UK or otherwise subject to the UK GDPR) and of the EU GDPR (regarding personal data collected in the EEA or otherwise subject to the EU GDPR). Other than that, transfers to the EEA are currently made under the relevant adequacy decision and transfers from the UK to the EEA do not require any specific safeguard by virtue of the Adequacy Decisions.

UK and EU Representatives

The Adequacy Decisions do not relieve UK-based controllers and processors from appointing an EU representative as is required under Article 27 EU GDPR if and to the extent that the EU GDPR applies to them.

One often-neglected consequence of the move to the UK GDPR is that a UK representative must now be appointed by a non-UK-based data controller or processor where it is subject to the UK GDPR. That requirement applies if the processing by a data controller or processor relates to the offering of goods and services to, or monitoring of, data subjects in the UK and the organisation is not established in the UK. There are exceptions from that requirement for occasional and small scale or non-special category processing which mirror that under the EU GDPR itself. The ICO is yet to publish any enforcement action it has taken in relation to the failure to appoint a UK representative.

4. International Transfers

Chapter V of the UK GDPR requires there to be appropriate safeguards for international transfers of data to outside of the UK. To the extent that a UK GDPR adequacy decision is unavailable, alternative safeguards are provided for under Article 46 of the UK GDPR. In addition, as the *Data Protection Commissioner v Facebook Ireland Limited & Maximillian Schrems* (Case C-311/18) ("**Schrems II** case was decided prior to the end of the Brexit transition period, it still applies as retained EU law, from which only the UK's

higher courts may diverge. This means that exporters must ensure that data receives "substantially similar" protections in the country importing the data to those available under the UK GDPR, including that enforceable data subject rights and remedies are available.

The ICO has proposed UK-specific transfer safeguards to fulfil the requirements of Article 46 of the UK GDPR. In particular, it has published a draft international data transfer agreement ("**IDTA**") (effectively a UK version of the EU's Standard Contractual Clauses ("**EU SCCs**")), for use when exporting personal data to a third country. There are distinct differences between the IDTA and the EU SCCs, from the "plain English" drafting of the IDTA down to the different types of transfer that each may cover.

Organisations subject to both the EU and the UK GDPR may wonder whether they will need to put in place two transfer safeguards for the same transfer. This is not necessarily the case, as the ICO has also published a draft short form "UK Addendum". This is intended to be used alongside the EU SCCs as an approved safeguard under the UK GDPR, in place of the IDTA. The UK Addendum makes minor amendments to the EU SCCs, to make them work in the context of the UK GDPR. The UK Addendum is likely to be commercially preferable to organisations that have already updated their EU SCCs within their data transfer agreements, because simply adding the UK Addendum will facilitate compliance with the UK GDPR without the full IDTA.

Alongside the IDTA, the ICO published a draft transfer risk assessment ("**TRA**"), which is designed to be used to fulfil the *Schrems II* requirement to assess transfer risks and to ensure equivalent protection is available before making a third country transfer. Again, the TRA takes a relatively different, arguably more pragmatic, approach to risk assessment, at least compared to the EDPB guidance on the topic.

UK to EU Transfers

At present, transfers from the UK to the EU are safeguarded by the Adequacy Decisions, adopted on 28 June 2021. To the extent that the Consultation proposes significant divergences by the UK from the EU GDPR, this may impact these Adequacy Decisions. This would of course introduce significant friction for EEA-UK data flows.

Updates to the EU SCCs and remediation

The Commission adopted the following two sets of EU SCCs in the context of the EU GDPR, that entered into force on 27 June 2021:

- EU SCCs replacing the old standard contractual clauses ("**Old EU SCCs**") providing appropriate safeguards within the meaning of Article 46(1) and (2)(c) of the EU GDPR for the transfer of personal data by a controller or processor (data exporter) to a controller or (sub-)processor whose processing is not subject to the EU GDPR (data importer); and
- EU SCCs that can be used in contracts between controllers and processors that process personal data on behalf of the controller(s) for compliance with the requirements of Article 28(3) and (4) of the GDPR, regardless of whether there is a transfer or not.

The main innovation in the EU SCCs for transfers of personal data to third countries reside in its modular structure giving the flexibility to cover various transfer scenarios within one single document, i.e. transfers from controller to controller, from controller to

processor; from processor to processor and from processor to controller. The same set of EU SCCs equally cover the rights and obligations of controllers and processors with respect to the requirements in Article 28(3) and (4) of the EU GDPR.

These EU SCCs for transfers notably reflect some requirements deriving from the EU GDPR as interpreted in the light of the outcome of Schrems II. Nevertheless, they do not remove the consequences of the CJEU ruling and the need to assess the necessity to adopt supplemental measures as recommended by the EDPB (in a version adopted for public consultation).

The Old EU SCCs were repealed on 27 September 2021. Contracts concluded before that day that rely on the Old EU SCCs will remain valid until 27 December 2022, provided the processing operations that are the subject matter of the contract remain unchanged and that reliance on the Old EU SCCs ensures that the transfer of personal data is subject to appropriate safeguards within the meaning of Article 46(1) of the EU GDPR.

5. Future Developments

UK's Approach to the ePrivacy Regulation

The ePrivacy Regulation, once finalised and implemented, will be EU law and thus not directly applicable as part of the UK data protection regime. However, the developments will be relevant for many UK companies that are likely to fall within its extra-territorial scope.

This may raise complex issues, as the UK Consultation also proposes amendments to PECR, which may conflict with the changes that are proposed in the current draft of the ePrivacy Regulation. For example, the Consultation proposes removing the requirement to obtain consent for analytics cookies and permitting websites to use "legitimate interest" cookies without obtaining consent for limited purposes.

It is also possible that the UK will not follow the EU's lead on the many other planned legislative developments, such as the proposed EU Regulation on Data Governance.

Organisations will therefore need to navigate a patchwork of data-related obligations that will apply across the UK and EU.

Authors:
Gary Cywie, *Partner*
ELVINGER HOSS PRUSSEN | garycywie@elvingerhoss.lu
Katie Hewson, *Partner*
STEPHENSON HARWOOD | katie.hewson@shlegal.com
Jonathan Howie, *Trainee Solicitor*
STEPHENSON HARWOOD | jonathan.howie@shlegal.com

→ 1. Opinion 14/2021 regarding the Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom, pt. 37 (available at https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf).

For any further information please contact us or visit our website at **www.elvingerhoss.lu**.

The information contained herein is not intended to be a comprehensive study or to provide legal advice and should not be treated as a substitute for specific legal advice concerning particular situations.

We undertake no responsibility to notify any change in law or practice after the date of this newsletter.