Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

End of Brexit Transition Period: Privacy Implications

January 8, 2021

The transition period following Brexit, during which a full status quo was applied in the relationship between the United Kingdom and the European Union, ended on 31 December 2020. At the eleventh hour, on 24 December 2020, the two sides concluded the EU-UK Trade and Cooperation Agreement (the TCA), outlining in principle the UK's future relationship with the EU. There are three issues in relation to data protection that businesses should be aware of in light of the TCA and the new UK-EU relationship.

1. The UK data protection laws

Regulation (EU) 2016/679, i.e. the EU General Data Protection Regulation (the EU GDPR), in its current form, has been retained as part of UK domestic law; and, in that current form, is now called the "UK GDPR." The UK GDPR sits alongside the UK Data Protection Act 2018, as amended. Other EU privacy laws, such as the ePrivacy Directive (Directive 2002/58/EC on privacy and electronic communications), have also been transposed into UK domestic law and will remain part of it.

This means that at present, UK organisations that, for example, are already EU GDPR compliant, are also compliant with the UK GDPR. For now, all of the main principles, obligations and rights remain the same under the two pieces of legislation. However, going forward, companies should continue to monitor developments in this area as the UK has the independence to amend the UK privacy law framework. The extent to which UK data protection laws will diverge from EU laws will depend, in part, on the terms of any further deal the UK reaches with the EU, in particular in relation to "adequacy" (see below).

2. Representative in the European Economic Area

Any businesses that are based outside the European Economic Area (in this alert, we will use "EU" to refer to the European Economic Area too, for ease) but are nevertheless within the scope of the EU GDPR have had to consider whether to appoint a so-called EU representative, as required under the EU GDPR. The role of the EU representative is to act on behalf of the business which has designated it in relation to that business's compliance with the GDPR: for example, the EU

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Jenny Arlington
Counsel
jarlington@akingump.com
London
+44 20.7012.9631

Jay Jamooji
Associate
Jay.jamooji@akingump.com
London
+44 20.7012.9845

representative serves as a point of contact for EU data subjects, and in the context of communications with the relevant EU data protection regulatory authorities.

If businesses have an establishment (i.e. office, branch, subsidiary, another legal entity) in the UK, they would have been within the EU prior to 31 December 2020, and no EU representative would have been necessary.

Now, international businesses that have an establishment in the UK and do not have any establishments in the EU, but are nevertheless within the scope of the EU GDPR, need to consider if an EU representative is required. In general, an EU representative is required unless certain exemptions apply. Businesses need to check therefore if they are within the scope of the EU GDPR and, if they are, whether any of the exemptions to appointing an EU representative apply. If not, one would need to be appointed.

3. Data flows between the UK and the EU

Under the EU GDPR, exporting personal data outside the EU is restricted. Such data transfers can only be carried out if certain requirements are satisfied. As the UK is no longer part of the EU, data transfers from the EU to the UK would therefore be restricted. The TCA concluded at the end of December 2020 regulates, on a short term basis, those data flows.

From the EU to the UK

The TCA provides for an interim continued, unrestricted flow of personal data from the EU to the UK until either:

I. 30 April 2021, which can be extended until 30 June 2021, by mutual agreement (the "additional transition period"); or

II. until the European Commission adopts an "adequacy" decision under Article 45(3) of the EU GDPR, i.e. a decision that UK data protection laws offer an adequate level of protection for personal data,

whichever is earlier.

The TCA confirms that for the duration of the additional transition period, the UK will not be treated as a "third country" under the EU GDPR, provided that, amongst other things, UK data protection laws do not change. In practice, this means that organisations in the EU that are already compliant with the EU GDPR can continue to transfer data to the UK, without the need to implement further safeguards during the additional transition period. Treating the UK as a "third country" would have meant that the restrictions on data flows apply, which would have created some obstacles for international businesses (see below).

From the UK to the EU

So far as transfers of data from the UK to the EU are concerned, the UK previously announced that it has deemed the EU Member States, Iceland, Liechtenstein, Norway and Switzerland to be adequate on a transitional basis, meaning that such transfers can continue. This decision will be kept under review by the UK government.

The UK government has also confirmed that UK organisations will be able to rely on the same mechanisms as under the EU GDPR to transfer data to a non-EU country,

including that the UK regime will recognise existing EU adequacy decisions; those currently relate to only 12 countries.

Next steps for international businesses

Without the six-month additional transition period agreed to under the TCA, businesses transferring data from the EU to the UK (which likely means most if not all international businesses) would have had to put alternative arrangements in place, such as carrying out an analysis of the lawful basis for their transferring data to the UK, adopting additional contracts or pausing the transfers until such steps were in place. The six-month period provides some welcome breathing space for international business.

The central question is whether the European Commission will be able and willing to complete its adequacy assessment of the UK's data protection laws within these six months. If the UK is granted "adequacy," data flows will continue unrestricted. However, if no "adequacy" is granted, businesses will need to implement significant changes to their contractual framework as well as their technical and operational procedures in order to carry out compliant international data flows.

Some questions as to whether the UK will achieve adequacy have been raised by recent developments (see our previous alert on recent EU Judgments, which have been critical of the UK's national security laws). The Information Commissioner's Office (the UK data protection regulator) has welcomed the TCA, but already announced that businesses should take precautionary steps in order to safeguard against any interruption to data flows in the event that no "adequacy" decision is reached. Such measures could include entering into the EU Standard Contractual Clauses (including the implementation of any necessary "supplementary measures"), implementing Binding Corporate Rules or relying on any of the available derogations in the EU GDPR. It seems like a busy start to the New Year from a data protection perspective.

akingump.com