ALSTON & BIRD

WWW.ALSTON.COM

Privacy & Data Security ADVISORY ■

DECEMBER 9, 2020

Brexit and Data Protection: What You Need to Know

by Wim Nauwelaerts and Paul Greaves

On December 31, 2020, the Brexit Transition Period is scheduled to come to an end, completing the protracted divorce between the UK and European Union. The EU General Data Protection Regulation (EU GDPR) will be brought into UK law as the 'UK GDPR' as part of a new body of 'Retained EU Law'. Although the UK GDPR will mirror the EU GDPR in many respects, there are key action points that companies may need to take to ensure continued compliance:

- Consider how EU-UK personal data transfers can continue in compliance with both EU and UK data protection law.
- Consider how personal data transfers from the UK to controllers and processors outside the EU (e.g., in the U.S.) can be legitimized.
- Review processing activities to continue to take advantage of the EU GDPR's 'one-stop-shop' mechanism (if available in the first place).
- Consider whether the company needs to appoint local representatives for EU and/or UK GDPR purposes.
- Assess how other compliance documentation and data protection provisions in agreements may be affected.
- Keep an eye on how the UK GDPR and EU GDPR may develop—and possibly diverge—over time.

Background

The UK officially left the EU on January 31, 2020. Since then, the UK has been in the 'Brexit Transition Period', designed to create a period of stability to enable the UK and EU to negotiate a new post-Brexit relationship. During the Brexit Transition Period:

- EU law (such as the EU GDPR) largely continues to apply in the UK.
- The UK is still considered for most purposes to be an EU Member State—meaning that the free flow of personal data continues between the UK and EU. The EU GDPR's restrictions on international transfers of personal data do not kick in for such transfers.

- The UK no longer takes part in EU decision-making. For example, the UK's supervisory authority (UK ICO) is no longer a full member of the European Data Protection Board.

During the Brexit Transition Period, companies have therefore largely been able to continue as normal—at least from a data protection perspective. However, things are about to change: the Brexit Transition Period is scheduled to end on December 31, 2020. After that date, the UK will be seen by the EU to be a 'third country', and EU law will no longer apply to the UK. In other words, the protracted divorce between the UK and EU will be complete.

The UK has, however, made some arrangements for the end of the Brexit Transition Period. The default position is that the UK will create a body of 'Retained EU Law', which takes certain EU legislation as it was at the end of the Brexit Transition Period and transposes it directly into UK law. As part of the Retained EU Law, the EU GDPR will be brought into UK law as the UK GDPR, which will be—at least initially—a mirror image of the EU GDPR (albeit with some tweaks so that it makes sense in a UK-only context). The UK Data Protection Act 2018 will continue to apply, supplementing the UK GDPR.

Companies with dealings in the UK and EU will therefore need to consider to what extent the UK GDPR and EU GDPR apply to them and what the impact will be once the UK is no longer considered an EU Member State for data protection purposes.

Potential Challenges for Businesses

Companies doing business in both the UK and EU face a wide variety of challenges associated with the UK's departure from the EU, but the main data protection action points that companies may need to take to ensure continued compliance are:

Consider how EU-UK personal data transfers can continue in compliance with both EU and UK data protection law

Under the EU GDPR, transfers of personal data from a controller/processor in the EU to a data recipient in a third country are in principle forbidden, unless the transfer is legitimized by a 'data transfer mechanism' as set out by Chapter V of the EU GDPR. Following the end of the Brexit Transition Period, the UK will be seen as a 'third country', and so companies transferring personal data to the UK will need to identify which data transfer mechanisms may be appropriate for their EU-to-UK transfers.

It is open to the European Commission to make a 'decision of adequacy' for the UK, which would allow for the free flow of personal data from the EU to the UK on the basis that the UK's laws offer adequate protections for personal data. In that case, companies do not need to put in place a data transfer mechanism themselves. However, it is far from guaranteed that the UK will qualify for a decision of adequacy (particularly in light of its national security laws). Even if the UK does qualify, it is not clear when the European Commission will be in a position to grant a decision of adequacy.

Absent a decision of adequacy or an interim solution agreed by the EU and UK governments, companies in the EU will need to identify and implement a suitable data transfer mechanism to legitimize their data transfers as of January 1, 2021. They may need to consider, for example:

- Whether they use the standard contractual clauses (SCCs) approved by the European Commission. Using SCCs also means that the data exporter and importer will need to conduct a transfer impact assessment and possibly implement supplementary safeguards, following the recent *Schrems II* judgment.
- Whether it makes sense to adopt binding corporate rules (BCRs) for intragroup transfers, or whether existing BCRs need to be amended.
- Whether they can rely on one of the derogations under Article 49 of the EU GDPR.
- Whether they can localize personal data within the EU, obviating the need for a data transfer mechanism.

On the other hand, the UK has made arrangements to treat EU Member States' data protection laws as 'adequate' from a UK perspective after the end of the Brexit Transition Period—meaning that companies can freely transfer personal data to the EU from the UK. However, these arrangements will be adopted on a 'transitional' basis and will be kept under review by the UK government.

Consider how personal data transfers from the UK to controllers and processors outside the EU can be legitimized

Considering that the UK will create a 'UK GDPR'—initially mirroring the EU GDPR—transfers from the UK to controllers and processors outside the UK (such as in the U.S.) will be in principle forbidden unless legitimized by a data transfer mechanism under the UK GDPR.

The data transfer mechanisms under the UK GDPR will reflect those of the EU GDPR. The UK has already made some preliminary arrangements for these data transfer mechanisms, which attempt to preserve the approaches that companies are already taking. For example:

- The UK will recognize decisions of adequacy that the European Commission has made for third countries (e.g., Switzerland and Israel).
- The existing SCCs approved by the European Commission can continue to be used to legitimize transfers outside the UK.

Again, these arrangements will be adopted on a 'transitional' basis and will be kept under review by the UK government.

Review processing activities to continue to take advantage of the EU GDPR's 'one-stop-shop' mechanism

One of the novelties of the EU GDPR when it came into force was that companies carrying out cross-border processing across more than one EU Member State may qualify for a mechanism that allows them to deal with only one lead supervisory authority in a single EU Member State, instead of 28 (soon 27) different authorities. The location of the lead supervisory authority depends on the location of the company's 'main establishment' in the EU. This is the so-called one-stop-shop mechanism.

However, following the end of the Brexit Transition Period, the UK ICO can no longer act as a lead supervisory authority. Companies that in the past had identified the UK ICO as their lead authority will need to consider their options. For example, they may need to:

- Consider whether they will continue carrying out cross-border processing activities.
- Identify any new lead supervisory authority in the EU, and potentially make initial contact.
- Review and change their operations to ensure that they continue to have a main establishment in the EU and can continue to take advantage of the one-stop-shop mechanism.
- Understand how the company's risk profile may change if it can be subject to parallel investigations or enforcement actions by the UK ICO and one or more EU supervisory authorities.

Consider whether the company needs to appoint local representatives for EU and UK GDPR purposes

If a company is not established in the EU but is subject to the EU GDPR under the EU GDPR's extraterritorial application provisions (e.g., a U.S. company targeting consumers in the EU with online products), then the company must typically appoint a representative in the EU for GDPR purposes.

The UK GDPR will mirror this requirement. As a consequence, companies captured by both the UK and EU GDPRs' extraterritorial application provisions after the Brexit Transition Period will in principle need to appoint representatives in both the UK and EU. These representatives will need to meet all the relevant requirements under the UK and EU GDPRs.

Assess how other compliance documentation and data protection provisions in agreements may be affected

Other compliance documentation, templates, and contractual provisions may need to be updated to reflect the fact that the UK is no longer considered to be part of the EU. For example:

- UK-specific privacy notices may need to be created (or existing privacy notices may need to be updated, for example to address transfers between the UK and EU).
- Data processing agreements, data transfer agreements, and other contractual provisions may need to be amended to reference the correct jurisdictions and to describe the correct data flows.
- The company's Article 30 records of processing activities and its GDPR data protection impact assessments may need to be updated to cover transfers of personal data between the UK and EU.

What About Future Developments in UK or EU Data Protection Laws?

Once the UK has fully separated itself from the EU, the UK government will theoretically be able to develop or change the UK data protection regime, and the UK will not be bound by subsequent judgments from the Court of Justice of the European Union (CJEU). UK courts may also develop or interpret data protection rules over time. The UK and EU data protection laws may therefore drift apart—increasing the compliance burden for companies operating across the UK and EU.

Following the end of the Brexit Transition Period, new GDPR compliance mechanisms adopted at an EU level (such as modernized SCCs or EU GDPR codes of conduct) may not necessarily be adopted in the UK.

To add a further layer of complexity, the EU-UK Withdrawal Agreement also contains a provision (Article 71(1)) that seeks to preserve the level of protection afforded to data subjects outside the UK where their personal data are:

- Processed under EU law within the UK before the end of the Brexit Transition Period ('legacy non-UK personal data').
- Processed within the UK on the basis of the EU-UK Withdrawal Agreement after the Brexit Transition Period ('Withdrawal Agreement data').

Article 71(1) provides that EU data protection law as it stood just before the end of the Brexit Transition Period (broadly speaking—'due regard' will be given to any subsequent decisions from the CJEU) shall continue to apply in the UK for legacy non-UK personal data and withdrawal agreement data after the end of the Brexit Transition Period. If UK data protection law starts to diverge from the data protection rules that apply under Article 71(1), companies may need to be in a position to distinguish any legacy non-UK personal data and withdrawal agreement data from other personal data. Article 71(1) ceases to apply, however, to the extent that the UK receives an adequacy decision from the European Commission—another reason why an adequacy decision would be welcomed by companies.

In short, companies doing business on both sides of the Channel should keep an eye out for developments to both UK and EU data protection laws and will need to seek out a commercial path for any divergences between the UK GDPR, EU GDPR, and potentially the rules that apply under Article 71(1) of the EU-UK Withdrawal Agreement.

You can subscribe to future ***Privacy & Data Security*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kelley Connolly Barnaby
202.239.3687
kelley.barnaby@alston.com

Kathleen Benway
202.239.3034
kathleen.benway@alston.com

Chris Baugher
404.881.7261
chris.baugher@alston.com

Alexander G. Brown
404.881.7943
alex.brown@alston.com

Elizabeth Broadway Brown
404.881.4688
liz.brown@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

David Carpenter
404.881.7881
david.carpenter@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Kimberly K. Chemerinsky
213.576.1079
kim.chemerinsky@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Maki DePalo
404.881.4280
maki.depalo@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

Stephanie A. Jones
213.576.1136
stephanie.jones@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Amy Mushahwar
202.239.3791
amy.mushahwar@alston.com

Wim Nauwelaerts
+32.2.550.3709
202.239.3709
wim.nauwelaerts@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Cara M. Peterman
404.881.7176
cara.peterman@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Jessica C. Smith
213.576.1062
jessica.smith@alston.com

Lawrence R. Sommerfeld
404.881.7455
larry.sommerfeld@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Richard R. Willis
+32.2.550.3700
richard.willis@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com