



**Brexit and GDPR: The impact of the new
deadline and practical steps to take now**

Deloitte North South Europe Privacy Services

July 2019

Brexit: The current outlook

The EU has granted the UK a Brexit extension

Following the passing of the original Brexit deadline on 29 March 2019, the EU has granted the UK a **Brexit deadline extension until 31 October 2019.**

EU Commission communication

In its 5th Brexit Preparedness Communication from June 2019, the EU Commission reiterated "that it is the responsibility of all stakeholders to prepare for all scenarios".

UK PM appointed

On 23 July 2019 the newly chosen Conservative Party Leader Boris Johnson was appointed as the UK Prime Minister.

Extended Deadline

If the UK Parliament does not agree upon a Brexit deal before the extended deadline, the UK will exit the EU without a deal (unless the EU agrees with another extension).

Data flows to and from the UK and the European Economic Area (EEA) could be seriously impacted by a no-deal Brexit or an agreement that **fails to compensate the effect of a Brexit** on personal data transfers.

Many organisations have already **invested heavily to achieve GDPR compliance**. A potential **no-deal Brexit** would require them to cope with **additional challenges** to ensure uninterrupted GDPR compliance.

Deloitte can assist your organisation with effectively fusing current and completed activities to Brexit-related activities, **enabling you to stay compliant and keep your business operational.**

Adequacy Post-Brexit

The UK stated that it will pursue “adequacy”. What is it and how can it be achieved?

What is 'Adequacy'?

The EU Commission (EC) has the power to determine whether a country outside of the EEA (a 'third country') offers an adequate level of data protection, through its domestic legislation or the international commitments it has entered into. If the EC decides this to be the case, the so-called 'Adequacy decision' removes the immediate need for businesses and organisations based in that country to adopt additional safeguards for personal data transfers to the country. After a no-deal Brexit, until the UK receives this adequacy status, it will be deemed a 'third country' to which no data transfers may take place without an alternative transfer mechanism (more about these on the next page).

Which countries are adequate?

As of June 2019, the EC recognises:

- Andorra
- Argentina
- Canada (commercial organisations)
- Faroe Islands
- Guernsey and Jersey
- Israel
- The Isle of Man
- Japan
- New Zealand
- Switzerland
- Uruguay
- The United States of America (Privacy Shield framework*)

Characteristics of adequacy

The process of adoption of an adequacy decision involves a number of steps and can be a lengthy process (possibly taking up to 21 months or more). The current understanding is that the adoption process can start after the UK leaves the EU, as is set out in the Political Declaration (dated 25 November 2018).

Adoption of an adequacy decision for the UK is not guaranteed. Moreover, the adequacy decision may be revoked by the EC (or annulled by the EU Court of Justice – e.g. Safe Harbour) after adoption. This depends on whether the level of data protection remains adequate from the perspective of EU law.



ICO's future

In any Brexit scenario, the British Supervisory Authority (Information Commissioner's Office (ICO)), will see its role as a member of the European Data Protection Board – including a role in the one-stop-shop mechanism – stripped away. This requires organisations that have the ICO as their lead Supervisory Authority to instead contact another Supervisory Authority, located in the EU.

The EU has said that the ICO can sit in on meetings which it holds post-Brexit, but will have no say. From an internal UK perspective, the ICO will still retain (most of) its functions and responsibilities post-Brexit.

* Privacy Shield framework refers to the self-certification scheme enabling USA organisations to transfer personal data from the EEA to the USA.

Alternative Transfer Mechanisms

Without relying on an Adequacy Decision, organisations can consider their options for compliance regarding personal data transfers to the UK



Binding Corporate Rules

What is it?

Binding Corporate Rules (BCRs) are an internal set of rules (policies) for data transfers within multinational companies. They allow multinational companies to transfer personal data internationally within the same corporate group to countries that do not provide an adequate level of protection.

Next to procedures for internal alignment, the establishment of BCRs includes a review of the BCRs by the lead Supervisory Authority.



The pros and cons

- BCRs are a strategic solution for a multinational organisation, allowing to a large degree control on the substantive rules across the globe.
- A straightforward BCR application can take 12 months or more to complete.
- Alternative safeguards might need to be in place in the meantime.
- BCRs are for internal data transfers between entities and cannot cover data transfers to third parties.



Standard Contractual Clauses

What is it?

The European Commission (EC) can decide that specific Standard Contractual Clauses offer sufficient safeguards for personal data to be transferred outside the EEA. It has issued such Standard Contractual Clauses for the following circumstances:

- EU controller to non-EU or EEA controller
- EU controller to non-EU or EEA processor



The pros and cons

- Standard Contractual Clauses are the easiest safeguard to implement.
- Review (and possibly amendment) of all data processing/transfer agreements between the EEA and UK will be required.
- Standard Contractual Clauses issued by the EC may not be amended by an organization wanting to use them. This can potentially lead to a suboptimal fit between the SCC and the business operations, thereby potentially requiring changes to the latter.



Other Mechanisms

What are they?

The GDPR provides other mechanisms for businesses to undertake for data transfers to third countries. Some of these mechanisms do need guidance and approval from the relevant Supervisory Authority.

It is recommended to closely evaluate their potential for your personal data processing instead of relying on them from the outset.



Derogations

These are for (one-off) transfers used under extraordinary scenarios such as explicit consent, or vital interests (e.g. to save a life).

Codes of conduct

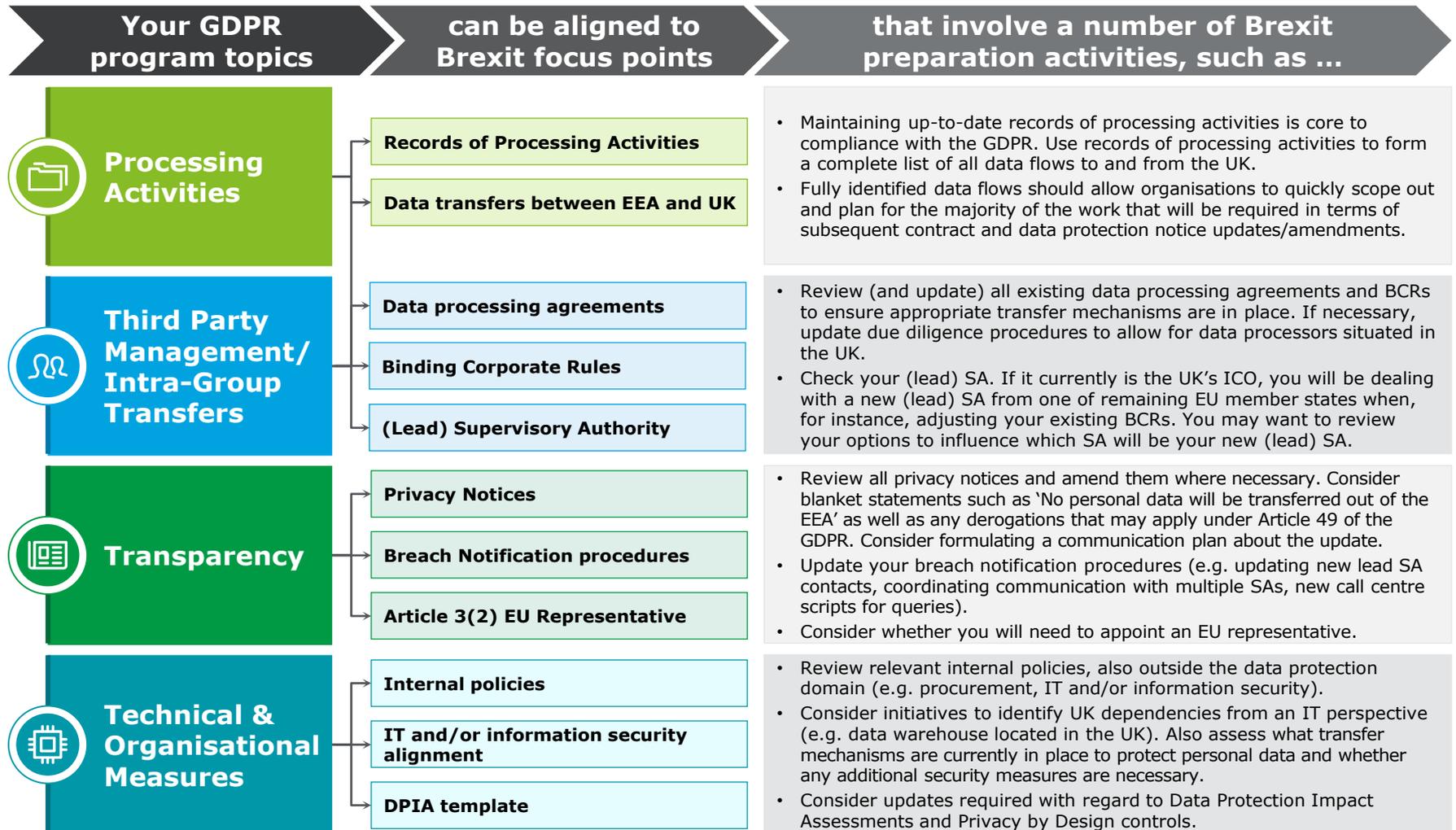
These are a set list of rules drafted by, e.g., an association which their members promise to follow across their entities.

Certification

There is the potential for some companies to take the workload of the Supervisory Authorities and be registered to declare companies adequate. At this moment in time, momentum is growing across the EEA in relation to certification bodies.

Aligning Brexit activities to your privacy program

A well-prepared action plan will facilitate a smooth transition and continuation of a free flow of personal data between the EU and the UK



Contact information

For more information, and support with your GDPR or Brexit programmes, please contact our Deloitte NSE Data Protection professionals:

Belgium

Erik Luysterborg

Partner



Risk Advisory
+32 497 51 53 95
eluysterborg@deloitte.com

Denmark

Line Perlman

Partner



Risk Advisory
+45 29 70 14 80
perlman@deloitte.dk

Finland

Hannu Kasanen

Director



Risk Advisory
+358 (0)50 5311 144
hannu.kasanen@deloitte.fi

Greece

Christos Vidakis

Partner



Risk Advisory
+30 2106781181
cvidakis@deloitte.gr

Iceland

Birna Sigurðardóttir

Partner



Risk Advisory
+354-8986460
birna.maria.sigurdardottir@deloitte.is

Ireland

Nicola Flannery

Senior Manager



Risk Advisory
+353 1 417 2665
niflannery@deloitte.ie

Italy

Tommaso Stranieri

Partner



Risk Advisory
+39 0283322630
tstranieri@deloitte.it

Malta

Ian Coppini

Partner



Risk Advisory
+356-23432444
icoppini@deloitte.com.mt

Norway

Bjørn Jonassen

Partner



Risk Advisory
+47992 27 420
bjjonassen@deloitte.no

Sweden

Peter Birgersson

Senior Manager



Risk Advisory
+46700802469
pbirgersson@deloitte.se

Switzerland

Maria Pisa

Senior Manager



Risk Advisory
+41 79 878 0123
mariapisa@deloitte.ch

The Netherlands

Annika Sponselee

Partner



Risk Advisory
+31 (0)88 2882463
asponselee@deloitte.nl

The United Kingdom

Peter Gooch

Partner



Risk Advisory
+44 (0)20 7303 0972
pgooch@deloitte.co.uk

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.nl/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte’s approximately 225,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2019 Deloitte North South Europe. All rights reserved.

Designed by CoRe Creative Services. RITM0295681