DataGuard

Whitepaper

GDPR AFTER BREXIT – WHAT IS CHANGING IN UK DATA PROTECTION?

TABLE OF CONTENTS

THE MOST IMPORTANT POINTS IN A NUTSHELL

- Brexit is impacting data protection compliance for businesses both across the UK and the EU
- The GDPR will remain applicable in the UK during the Brexit transition period until 31 December 2020, after which it will become a "third country"
- With an adequacy decision, the EU Commission could put the UK on an equal footing with EU countries in terms of data transfers
- This requires the UK to continue to adhere to EU standards on data protection and it remains unclear if the EU Commission will grant adequacy at the moment
- Regardless, companies need to take many measures to prepare for the end of the Brexit transition period as soon as possible
- Answers to the questions surrounding the data protection implications of Brexit can be provided by your data protection officer (DPO), external consultants and the British authorities

---

The Brexit transition period is coming to an end and it is foreseeable that the impact of this could be severe. Companies should focus on the topics of GDPR and data protection in order to continue to ensure compliance with applicable data protection law.

In this whitepaper, you will learn more about the current situation in the wake of the United Kingdom's withdrawal from the European Union. We will discuss the issues that are most relevant to both EU & UK businesses post-Brexit, with a focus on becoming and remaining privacy compliant under the data protection rules and regulations when doing business with the European Union.

WHAT HAPPENS AFTER THE BREXIT TRANSITION PERIOD?

During the Brexit transition period, the General Data Protection Regulation (GDPR) will remain applicable in the UK without change.

After the end of the Brexit transition period on 31 December 2020, the UK will become a so-called "third country" and the GDPR will apply as it would in any other third country, ceasing to apply to UK entities that fall outside the extraterritorial scope of application. This means that data transfers to a company in the UK from the EU, regardless of whether it is, for example, a separate establishment or a service provider, require a specific legal basis. GDPR regulates international transfers of data under its Chapter 5 and includes the following transfer mechanisms:

- An **adequacy decision** is granted when a country is determined to have an adequate level of data protection by the EU Commission. Regulated under Article 45(3) of the GDPR, an adequacy decision is granted by the EU Commission to confirm that a third country has a level of data protection comparable to EU standards. Data transfers to such a country are privileged as they do not require any additional transfer mechanisms. Currently, adequacy decisions exist for the following third countries: Andorra, Argentina, Faroe Islands, Israel, Japan, Canada, New Zealand, Switzerland, Uruguay as well as the British Isles of Guernsey, Isle of Man and Jersey, which are not part of the United Kingdom as crown ownership.
- **Binding Corporate Rules (BCRs)** are an appropriate safeguard to carry out international data transfers and bind various entities of a worldwide corporate group while granting enforceable rights to the data subjects. They ensure the same high level of protection of personal data is complied with by all members of the organisation. BCRs must be approved by the supervisory authority, however, this has proven difficult in the past as few organisations have had BCRs successfully approved to this date.

- **Standard Data Protection Clauses** are standard contractual clauses (SCCs) adopted by the EU Commission or a supervisory authority and executed between a data exporter and a data importer. Recital 109 of the GDPR encourages controllers and processors to provide additional safeguards via contractual commitments that supplement these standard data protection clauses. SCCs are mechanisms by which organisations can commit to protect personal data when engaging in cross-border data transfers.

If one of the above mechanisms for transferring data is not possible, a cross border data transfer may take place following one of the conditions laid down under Article 49 of the GDPR "Derogations for Specific Situations". These specific situations include for example, transfers under explicit consent or for the necessary performance of a contract. Furthermore, the conditions set under Article 49 of the GDPR should be met under exceptional situations and not become a repetitive course of action. With this in mind, the UK government has put amendments in place that seek to achieve an adequacy decision.

As part of the transition agreement, the UK government has already incorporated the GDPR into local law with what has come to be known as the "UK-GDPR" in order to secure an adequacy decision from the EU Commission. The "UK-GDPR" sits alongside the Data Protection Act 2018 and with the Privacy and Electronic Communications Regulations (PECR), will make up the local privacy landscape after the transition period.

However, uncertainty looms in the UK as certain political figures have shown signs of a possible shift away from EU privacy standard. Previous remarks from the UK prime minister and the recently published national data strategy hint at the possibility of more "relaxed" and potentially insecure approach to data (see table on page 7). Though the UK at the moment seems to prioritise achieving an adequacy decision (scenario A) with the application of the UK-GDPR post-Brexit, we cannot exclude an alternative scenario (scenario B).

In any case, and as mentioned above, the GDPR will continue to be relevant to many companies in the UK. According to Article 3 of the GDPR, the regulation also applies to organisations in third countries which:

- Process personal data in the context of the activities of an establishment in the EU
- Offer goods and services to data subjects in the EU or
- Monitor the behaviour of individuals within the EU (e.g., via online tracking).

WHAT DOES IT MEAN IF THE UK BECOMES A THIRD COUNTRY?

After Brexit was introduced, the European Commission and the UK government have been engaging in formal negotiations to reach an adequacy decision. Despite both sides meeting several times, there is still no agreement to date, and considering other situations like Japan´s adequacy decision, the time to reach this decision might extend beyond the transition period. If the UK becomes a third country at the end of the transitional period, it will affect the way in which companies have to organise their data flows. Therefore, organisations should first check their data flows in relation to EU – UK data transfers.

The extent of changes that will be required in companies will depend on whether or not the European Commission will consider the level of data protection in the UK to be adequate. Whether this adequacy decision will exist is still unclear.

It is likely that this decision will be substantially dependent on the compatibility of the GDPR with surveillance rules such as those enshrined in the Investigatory Powers Act. Doubts about compatibility have grown since the European Court of Justice overturned the EU-US Privacy Shield in a landmark ruling in mid-July 2020, in which it deemed US surveillance laws incompatible with EU data protection standards.

Until the EU Commission has made an adequacy decision – or if it does not reach one at all – companies will have to meet special requirements for their data protection compliance. These can be found in Chapter 5 of the GDPR. With this in mind, the UK government has confirmed that data transfers from the UK to the EEA and other countries with an adequacy decision will not be restricted. In addition, the relationship between regulators will change after Brexit, as the Information Commissioner's Office (ICO) will no longer be an EU supervisory authority. Depending on how companies process their data, they may have to communicate with both the ICO and an EU supervisory authority for data protection in the future. The ICO recently issued two high profile fines on British Airways (20M GBP) and Marriot (18.4M GBP).

HOW CAN BUSINESSES PREPARE FOR THE END OF THE BREXIT TRANSITION PERIOD?

Companies should start preparing now in order to be able to operate in accordance with the rules after the Brexit transition period ends on 31 December 2020. Here is an overview of the possible measures and actions to take, which we will discuss in more detail below:

1. Check the data flows in the company, especially regarding transfers to and from the EU and the UK
2. Prepare by continuing to comply with GDPR privacy standards and verify with your DPO or privacy specialist how this impacts your organisation
3. Check if you need to appoint a representative in the UK or the EU
4. Consider that you may need to appoint a DPO in the UK and the EU
5. Review all contracts with suppliers, service providers and other parties in relation to EU and UK data transfers
6. Apply appropriate safeguards for international data transfers, such as BCRs and SCCs
7. Track what recommendations regulators such as the ICO give in relation to changes in data protection. The ICO has released guidance on how British organisations should handle data protection and data flows once the Brexit transition period ends

It is possible that the UK will turn away from EU data protection standards in the future. Although this is unlikely at the moment, it should not be excluded as a possible scenario (see table).

Regardless of which of the scenarios you are preparing for, keep in mind that implementing some measures can be time consuming. Many organisations fear a rise in compliance costs and burdens as privacy requirements may increase for those required to comply with both the GDPR and the UK privacy framework by the end of the transition period.

In order to prepare themselves concretely, companies in the UK and the EU should first review their data flows. This will allow them to determine directly whether Brexit affects them in terms of data protection at all and what they may need to change.

In addition, companies should consider whether they need a representative and a DPO in the UK (see points 4 and 5 on previous page). For which of the various envisioned scenarios this is the case, refer to our table below.

POST-BREXIT SCENARIOS

Scenario A: The UK continues the GDPR standard following the transition period with a national privacy framework (UK-GDPR & Data Protection Act 2018).

Scenario B: The UK decides to take a different approach to privacy, drifting away from EU standards.

DIFFERENT CASES THAT COULD OCCUR

Case 1:
The European Commission grants the UK an adequate level of data protection (adequacy decision) before the end of the transition period.

Case 2:
The European Commission grants the UK an adequate level of data protection (adequacy decision) after the end of transition period.

Case 3:
The European Commission denies the UK an adequacy decision (the UK is treated as a third country).

Case 4:
The UK decides to divert from the GDPR in favour of a "pro-business" approach under the new national data strategy or similar.

WHAT DOES THIS MEAN?

Transfers between the UK & the EEA can continue to operate without additional safeguards.

WHAT DOES THIS MEAN?

- Appropriate safeguards must be implemented for transfers from the EU to the UK (SCCs, BCRs, etc.).
- The EU Commission could point at necessary additional amendments to the national law before an adequacy decision is granted.

REGARDLESS OF THE SCENARIO OR CASE, ORGANISATIONS SHOULD CONSIDER THE FOLLOWING:

- Appointment of an EU/UK representative may be required.
- The ICO will no longer be recognised as a supervisory authority in the EU. It must be replaced by a supervisory authority in the EU for UK organisations processing data or with an establishment in the EU.
- It may be necessary to notify the appointment of a DPO in both the UK and the EU.

Note: The scenarios, cases and consequences mentioned are for illustrative purposes and based on DataGuard's assessment and are subject to change.

The best option to secure the transfer of data to the UK in the future are SCCs. By supplementing your Data Processing Agreement, you can prepare for data transfers to the UK if there is no adequacy decision.

For contracts with suppliers, service providers and other UK/EU parties, you should review and, if necessary, adjust the privacy clauses to be on the safe side regarding data protection.

Many post-Brexit requirements have not yet been definitively defined. Therefore, you should observe the recommendations for action given by the relevant supervisory authorities on this issue. You should also keep a close grip on the news of the impact of Brexit on data protection.

WHO CAN I CONTACT IF I HAVE QUESTIONS ABOUT DATA PROTECTION AND BREXIT?

The first point of contact for all questions about Brexit is certainly your company's DPO, for whom Brexit is probably part of the day-to-day business at the moment. So, he or she is likely to be able to answer most of the questions.

It may also be advisable to contact an external consultant. Here, you should make sure that he or she has international expertise, experience and presence in order to be able to provide you with the best possible support on this cross-border topic.

Another good alternative is the British institutions. For example, the Information Commissioner's Office (ICO) regularly issues guidance on topics including Brexit, data protection and the GDPR. Through Companies House the UK Government may also provide assistance to companies.

CONCLUSION: HOW WILL BREXIT AFFECT DATA PROTECTION COMPLIANCE ACROSS THE UK AND THE EU?

As we have seen, Brexit could have a serious impact on data protection for both UK and EU companies, especially when it comes to data flows and transfers. Many questions remain unanswered as the EU Commission has not yet issued an adequacy decision for the UK and it seems as if this will drag beyond close of the Brexit transition period at the end of the year. With this proving to be a continuously evolving landscape, we recommend that companies implement the safest necessary measures, so they are not caught by surprise at the turn of the year.

Questions about compliance with GDPR or searching for an external data protection officer?

At DataGuard, our certified privacy experts are here for you at eye level. Book your free consultation with an industry expert today and get to know us personally.

DataGuard is a Compliance software company focused on Data Privacy and Information Security. As a European leader in the Compliance SaaS category, we enable over thousands of SMB and Corporate customers to automate and operationalise Privacy, InfoSec, and Compliance ("PIC") with ease. Our end-to-end SaaS solution drastically reduces the time and money companies spend to comply with privacy legislation such as GDPR, manage consents and preferences, and obtain infosec certifications such as ISO 27001. This enables our customers to focus on their core business, create value through trust and compliance, whilst mitigating risks and preventing breaches. We have offices globally in Munich, Berlin, London, and Vienna.

Let's talk about your challenges and define first steps on your compliance journey:

Contact us

You might also like:

→ **GDPR Documents Checklist**

→ **The 6 most common Privacy Mistakes**

→ **On-Demand Webinar: Bullet proof privacy in the UK**

dataguard.co.uk contact@dataguard.com +44 20 3514 65 57

DataGuard