Published on *The National Law Review* https://natlawreview.com

How Will Brexit Affect the GDPR's Governance Over the UK?

Article By:

Chanley T. Howell

Steven Millendorf

Thomas E. Chisena

Since the referendum to leave the EU rocked the UK in 2016, commentators, privacy personnel, and corporate officers alike have been speculating as to how Brexit will affect Britain's subjugation to the General Data Protection Regulation 2016/679 (GDPR) and other EU privacy laws. The impact of Britain's withdrawal from the EU will be largely dependent on what exit deal, if any, ultimately passes British Parliament and is accepted by the EU. As British companies (and companies that market in Britain) have spent considerable time, effort, and money to become GDPR compliant, the uncertainty of the effect of the law moving forward has left many privacy and IT personnel worried of what new legal regimes will be next, especially because the details of the ultimate withdrawal deal remains anyone's guess. In this article, we outline the possibilities for the GDPR post-Brexit and provide some guidance on what the aftermath may look like.

What Would Britain's Relationship to the EU Look Like Post-Brexit?

To understand the application of a broad EU-based law (such as the GDPR) to a post-Brexit Britain, it is helpful to look at the possibilities for the UK's relationship to the EU after it no longer is a Member State. First, even if the UK withdrawals from the EU, it could be granted membership to the European Economic Area (EEA) trade group – similar to the relationship between Norway and Iceland and the EU. The EEA adopted the GDPR in July 2018, so in the case of EEA membership, the use of personal data in Britain would still be governed by the GDPR. Given that one of the stated reasons for Brexit was to break free of the rules and regulations of the EU and the EEA, it is unlikely that the UK will join the EEA, so this model seems doubtful.

If Britain does not join the EEA post-Brexit, even if it does join the legally more relaxed European Free Trade Association (EFTA), then the GDPR will not directly govern over the UK. This is the relationship that Switzerland has with the rest of the EEA. Britain joining only the EFTA and not the EEA seems to be most probable given the recent political commentary from Europe. If this is the case, data protection regulations and compliance requirements post-Brexit are more unclear.

Data Protection After a No-Deal Brexit

If Britain leaves the EU with no withdrawal agreement in place, or crashes out of the EU, the GDPR will no longer be binding on the UK effective from the date it leaves the EU. However, even if the GDPR will no longer directly govern over the UK, it is important to understand that any British company that has personnel in the EU or will continue to market or track EU citizens will still need to keep GDPR compliant for the processing of those EU individuals' data. Also, even if the GDPR is no longer binding on Britain, the UK's adopted versions of the laws (including the UK's Data Protection Act of 2018 (DPA)) will continue to remain in full force and effect. As the DPA was drafted to substantially mirror the GDPR, processing, transfer, and security requirements for British citizens' personal information will be substantially the same post-GDPR at least for the time being.

Where the greatest post-GDPR effects will be felt in a crash scenario is with the transfer of EU citizens' personal data out of the EU. Under the GDPR, Member State companies may freely transfer personal information between Britain and the rest of the EU without need for any additional legal mechanism to do so. However, in the case of a no-deal Brexit, this privilege will disappear, and the UK will need to implement and rely on standard contractual clauses or binding corporate rules (BCRs) to process any EU citizen's personal data in the UK. As these mechanisms may not currently be in place for all British companies, this could substantially delay and slow British data processing operations. Also, as consent is permissible from EU customers for certain data transfers, it rarely is permitted for the transfer of employee personal data. Thus, companies with operations in both the UK and the rest of the EU should begin thinking now about how to effect the transfer of employee data between the EU and the UK.

As an important note, after the UK leaves the EU, the EU could grant an "adequacy decision" to the UK. Under an adequacy decision, personal data can be freely transferred without the need for additional legal mechanisms between the EU and the *adequate* country (known as "Third Counties" under the GDPR) because the EU has determined that that country's data protection laws are sufficient to not degrade or diminish the legal protections for personal data under the GDPR. Third Countries include Canada, Israel, Switzerland, Japan, and Argentina. The U.S. is noticeably absent from this list, which is why transfers to the U.S. must be pursuant to a permitted transfer mechanism such as Privacy Shield or a Data Processing Agreement with EU-approved language. Given the closeness of Britain's DPA to the GDPR, an ultimate adequacy decision for the UK seems possible, but it will take some time to achieve. The designation of a Third Country requires a proposal from the European Commission that is then voted on by Member States. If Britain crashes out of the EU, EU Member States may not be too willing to extend this privilege to the UK.

While the transfer of personal data between the EU and the UK may become more complicated under a no-deal Brexit, the transfer between the U.S. and the UK will initially be largely unaffected. The UK will likely continue to transitionally recognize the existing EU standard contractual clauses, BCRs, and the EU-U.S. Privacy Shield. U.S. and British companies will likely just need to update their privacy policies and implement some minor tweaks to data protection policies. However, in the long run, the UK and the U.S. may have to negotiate their own version of Privacy Shield, and the UK will have to adopt its own version of the standard contractual clauses and requirements for BCRs, which may result in additional work for U.S. companies.

Data Protection If an Exit Deal Is Reached with the EU

While there is much speculation as to what the ultimate deal between the UK and the EU will be, the UK's current proposed draft sheds some light on what the ultimate goals are for Britain and personal data protection. The draft withdrawal agreement sets forth a transition period through December 31,

2020, where EU laws (including the GDPR) will continue to apply and the EU has agreed to not treat British data processed in the EU any differently because the UK has left. Specifically, the GDPR will continue to apply to personal data processed before or during the transition period (and for EU citizens' data after the transition period that was collected before it ended).

Throughout the transition period, the UK will be free to draft and explore potential personal data policies and legislations of its own, such as data transfer treaties with the U.S. and Canada, but such legislation may not go into effect until after the transition period ends. Also during the transition period, the EU will consider the appropriateness of an adequacy decision (as explained above) for the UK. At the end of the transition period or if an adequacy decision is not granted, the UK would be free to create new laws that differ from the GDPR as to how British and EU citizens' data is handled (except as otherwise explained above for data collected before the transition period ended or if the British company is otherwise subject to the GDPR because of the scope of its operations). As there is no guarantee that this legislation will pass Parliament or that it will be accepted by the EU, it is still uncertain whether these terms will come into effect.

Conclusion

As of the publishing of this article, the UK and the EU do not seem close to accepting a mutually agreed to withdrawal agreement. Accordingly, the GDPR's ultimate application for Britain moving forward remains uncertain. We will continue to monitor the situation and provide updates on potential outcomes for British privacy law as they develop. Likely, given the close connection between UK companies and other EU member states, there are strong economic and operational reasons to keep British privacy laws uniform with the GDPR post-Brexit. We shall see.

National Law Review, Volumess IX, Number 140