KYRIAKIDES GEORGOPOULOS
LAW FIRM



DATA PROTECTION PRACTICE

# The Data Protection Implications of Brexit

January 13, 2021

# The Data Protection Implications of Brexit

BY IRENE KYRIAKIDES, ELINA GEORGILI, NATALIA SOULIA

The latest massive developments in the field of cross border data transfers, evolving around the impact of CJEU Schrems II Judgement and Brexit, have become the most heated topic amongst privacy practitioners. UK withdrawal from the EU which took place on January 31, 2020, came into substantive effect after the end of the Brexit transition period agreed under the Withdrawal Agreement, on December 31, 2020. In terms of privacy, this means that beginning January 1, 2021 typically the UK does no longer apply directly the EU General Data Protection Regulation ("GDPR") as such and has become a third country as per Article 44 GDPR.

One of the major implications of Brexit in the area of data protection would be that, in the absence of an adequacy decision from the European Commission, any exchange of personal data between EEA stakeholders and UK entities would, as a rule, constitute in the post Brexit age a transfer of personal data to a third country and would be therefore subject to the provisions of Chapter V GDPR. Nonetheless, according to the Trade and Cooperation Agreement (also in summary here) (the "TCA"), which was concluded on December 24, 2020 and sets the entire framework for the UK's relationship with the EU, personal data flows between the EU to the UK will continue unhindered and uninterrupted for a further short term, without the need for additional safeguards. In any case given that the TCA provides only a temporary reprieve, the persisting question as to how will the data processing landscape develop after Brexit remains.

## I. Key takeaways of the TCA in relation to data protection

Whilst the TCA does not provide assurance that the UK provides an adequate level of protection for personal data, noting the importance of facilitating new opportunities for businesses and consumers through digital trade, and addressing unjustified barriers to data flows and trade enabled by electronic means (preamble of the TCA), it does come up with a temporary ad hoc contractual solution to deal with the upheaval Brexit brought, primarily intended to allow time for the European Commission to complete its adequacy assessment of the UK.

The "bridging mechanism" set up by the TCA (Article FINPROV.10A) enables the unrestricted free flow of personal data from the EU/EEA to the UK for an interim period commencing 1st January 2021 and lasting until the earlier of (i) the date on which the European Commission adopts an adequacy decision in respect of the UK under Article 45(3) of the GDPR, or (ii) 30 April 2021 (or 30 June 2021, if the EU has not issued an adequacy

decision by 30 April 2021, unless either the UK or the EU object to this). Transfers of personal data from the EU/EEA to the UK will not be considered transfers of personal data to a third country during this period, provided that the UK does not materially amend its current data protection rules (unless in alignment with the EU data protection law) and does not exercise certain powers (including approving new SCCS or binding corporate rules), without approval from the newly formed the UK/EU Partnership Council.

## II. Next steps for organisations

Businesses with an establishment in the UK or subject to UK data protection law should carefully take account of the following considerations:

### 1. Use alternative data transfer mechanisms

The CTA is considered to pave the way for an adequacy decision. In the Joint Declaration on the Adoption of Adequacy Decisions with Respect to the United Kingdom published alongside the TCA, the European Commission affirmed its intention to promptly launch the procedure for the adoption of an adequacy decision. Moreover, the UK statutory data protection framework comprises of the GDPR, which was incorporated, subject to certain amendments, into domestic UK law by virtue of the European Union (Withdrawal) Act 2018 (now referred to as "UK GDPR"), the UK Data Protection Act 2018 as well as the national implementing rules of other EU privacy legislation and, thus, mirrors to a large extent the EU framework. On this basis, it is hoped that the European Commission will grant formal data protection adequacy status to the UK, which would permit the ongoing free transfer of personal data from the EU to the UK, without requiring organizations to take any further steps.

However, it cannot be guaranteed that an adequacy decision will be reached and that the adequacy assessment of the UK's data protection laws will have been completed before the end of the interim period. In that event, transfers of personal data from EU/ EEA to the UK will take place in accordance with the requirements of Chapter V of the GDPR. Therefore, UK government and UK Information Commissioner's Office (the "ICO") recommend that UK-based organizations start taking precautionary steps to safeguard against any future interruption to the free flow of personal data between the EU and the UK, by putting alternative transfer arrangements in place.

It should be noted that with respect to data transfers from UK to the EU/EEA, Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 already stipulate that EU/ EEA provide adequate protection to personal data and hence transfers from UK to the EU/EEA will remain unaffected without requiring additional measures.

### 2. Ensure GDPR compliance

As of 1st January 2021, UK organisations which are caught by the extraterritorial reach of the GDPR, will have to achieve compliance both with the EU and the UK GDPR. For now, given that those two pieces of legislation coincide to a large extent, the position with regard to data processing essentially remains the same as under the previous regime and thus no further action to ensure legal

compliance in the area of data protection is required. However, as in the course of time EU and UK privacy laws will start to diverge, UK companies are advised to closely monitor EU legal requirements.

### 3. Consider how to benefit from the One-Stop-Shop mechanism

Following the end of the transition period, the ICO no longer forms part of the GDPR One-Stop-Shop mechanism. Organisations with establishment in the UK are, therefore, no longer able to use the ICO as their lead supervisory authority to handle cross-border processing and related complaints. The EDPB notes in its Statement on the End of the Brexit Transition Period that organisations whose main establishment is currently in the UK should consider whether to set up a new main establishment in the EEA following the end of the transition period in order to benefit from the One-Stop-Shop mechanism.

### 4. Appoint a Representative in the EU

EDPB emphasizes also that any businesses that have an establishment in the UK, but fall nevertheless within the scope of the EU GDPR, by virtue of offering goods or services to individuals in the EEA and/or monitoring the behaviour of individuals in the EEA, may have to appoint a so-called EU representative, as required under Article 27 GDPR.

It should be stressed that the UK GDPR imposes a similar obligation to appoint a UK representative to organisations which although not established in the UK hold and process data in respect of a data subject in the UK.

### 5. Appoint a DPO in the UK

Given that UK and EU DPO requirements are the same, companies under an obligation to appoint a DPO in the UK pursuant to UK data protection law, may appoint their EU DPO also as DPO for the UK territory, provided the DPO is easily accessible from both the UK and the EU.

### 6. Validate BCRs

Companies will need to resubmit their already approved Binding Corporate Rules ("BCR") to the ICO for validation, if they were approved by a supervisory authority other than the ICO, while new BCRs intended for use under both the UK and EU GDPR shall be approved both to the ICO and the competent supervisory authority in the EU.

### 7. Update documentation

Any changes in the applicable law and the obligations stemming therefrom shall also be reflected in Privacy notices, internal policies, contracts and other documents, which are required to be amended accordingly.

# Contact Us




Irene Kyriakides
**PARTNER**
*i.kyriakides@kglawfirm.gr*



Elina Georgili
**PARTNER**
*e.georgili@kglawfirm.gr*


*Follow Us*


**ATHENS OFFICE**

28, Dimitriou Soutsou Str.,
115 21 Athens

T +30 210 817 1500
F +30 210 685 6657-8
E kg.law@kglawfirm.gr

**THESSALONIKI OFFICE**

17, Ethnikis Antistasseos Str.,
551 34 Thessaloniki

T +30 2310 441 552
E kg.law@kglawfirm.gr


*www.kglawfirm.gr*


**Disclaimer**: This newsletter contains general information only and is not intended to provide specific legal, or other professional advice or services, nor is it suitable for such professional advice, and should not be used as a basis for any decision or action that may affect you or your business. Before making any decision or taking any action that may affect you or your business, you should consult a qualified professional advisor. We remain at your disposal should you require any further information or clarification in this regard.

**©Kyriakides Georgopoulos, 2021**