NO-DEAL BREXIT AND ITS LIKELY IMPACT ON TRANSFERS OF PERSONAL DATA BY EU-BASED ENTITIES TO THE UK

The UK formally left the EU on 31 January 2020, and its membership will be terminated at the end of the transition period on 31 December 2020 at midnight CET. The EU and the UK are currently negotiating and will need to come to an agreement on the future of their relationship by that date, or face a "cliff-edge" scenario: a no-deal scenario (i.e. no agreement about the "divorce" process) ("**No-deal Brexit**"). From a data protection standpoint, in case of a No-deal Brexit, the UK will become a "third country" within the meaning of the EU General Data Protection Regulation ((EU) 2016/679) ("**GDPR**"). The effect of such a change of status, is that data transfers will no longer be considered as intra-EU transmissions of data. In other words, personal data will no more flow from the European Economic Area ("**EEA**") to the UK without additional safeguards.

Key issues

- The UK formally left the EU on 31 January 2020, and its membership will be terminated at the end of the transition period on 31 December 2020 at midnight CET, thus becoming a third country.
- EU-based entities will need to legitimate the transfer of personal data to the UK according to the GDPR.
- In the absence of an adequacy decision, the most pragmatic way for EU-based entities to transfer data to UK-based entities could be the adoption of standard contractual clauses between the relevant EU and UK entities, or BCRs.
- Clifford Chance is organising a webinar on Thursday 24 September 2020 taking a global business perspective on the effects and main takeaways of the Schrems II case on international transfers of personal data.

LEGITIMATE DATA TRANSFERS TO THE UK IN CASE OF A NO-DEAL BREXIT

The GDPR aims at guaranteeing the free flow of personal data inside the EEA, while in principle prohibiting transfers of personal data to third countries located outside the EEA, which are not considered as providing an adequate level of data protection ("**International Data Transfers**").

In case of a No-Deal Brexit, from 1 January 2021 on, the UK will cease to be a member of the EU and will be considered as a "third country" for data protection purposes. Consequently, transfers of personal data to the UK – which currently do not require any justification or further safeguards will, from 1 January 2021, be considered as International Data Transfers.

The European Commission has the power to determine, on the basis of the GDPR, whether a country outside the EEA offers an adequate level of data protection by adopting an adequacy decision.[1]

International Data Transfers to countries for which the European Commission has adopted an adequacy decision do not require the implementation of any

[1] The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay as providing adequate protection. Prior to the Schrems II case which invalidated the Privacy Shield, the United States of America (limited to the Privacy Shield framework) were also recognised as providing adequate protection.

further safeguard. Although the UK would in principle present sufficient data protection guarantees, it is rather unlikely that, in case of a No-deal Brexit, such an adequacy decision be swiftly adopted by the European Commission.

In the absence of such an adequacy decision, the EU-based entities must therefore be in a position to legitimate their International Data Transfers to the UK, using one of the legal mechanisms provided for in the GDPR: standard contractual clauses adopted by the European Commission ("**SCCs**"), binding corporate rules ("**BCRs**"), codes of conduct or certification mechanisms.

Relying on derogations for specific situations (where the above mentioned mechanisms cannot be used), using for instance the data subject's consent or the performance of a contract concluded in the interest of the data subject(s) conceivable in theory, but should be, from a practical perspective, avoided to the maximum extent possible.

SCCs cannot however be used in all instances. The main takeaway from the CJEU's ruling in Case C-311/18 (so called "Schrems II" case) is that SCCs may not be relied upon if the third country entity importing the personal data cannot, by virtue of its national law, comply with the SCCs. In our opinion, this would not be the case of the UK, since UK's legal framework for data protection[2] is based on EU law the enforcement of which is monitored by an independent supervisory authority[3].

HOW TO PREPARE

In light of the uncertainties around the outcome of the negotiations at the end of the transition period, EU-based entities transferring personal data to the UK should anticipate a No-deal Brexit and put in place the necessary and appropriate measures to legitimate their transfers of personal data to the UK in compliance with the GDPR (relying on one of the grounds presented above).

In most situations, the most appropriate tool would be the SCCs. Different sets of SCCs are available on the European Commission's website[4] depending on the role of the UK entity receiving the personal data (either as a Data Controller or a Data Processor).

Clifford Chance is organising on Thursday 24 September 2020 a Webinar on the effects and main takeaways of the Schrems II case on international transfers of personal data, taking a global business perspective from different counsels of Clifford Chance offices from London, Brussels, Paris, Amsterdam and Washington. Do not hesitate to reach out to us should you be interested in knowing more about the implications of the Schrems II case.

Clifford Chance operates a global cross-practice group of lawyers specialising in data protection and related "data management" issues. We are uniquely placed with deep litigation experience and relationships with data protection authorities, to support clients through complaints, claims and investigations relating to data privacy and other issues across their businesses. This includes strategic advice as to the approach to be taken, design and implementation of compliance programmes and advice on ad hoc issues arising in the application of those programmes, such as the legitimisation of International Data Transfers.

[2] UK's legal framework for data protection is notably composed of the GDPR tailored by the Data Protection Act 2018, as well as other pieces of legislation such as privacy and electronic communications regulations.
[3] Information Commissioner's Office (ICO): https://ico.org.uk/
[4] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

CLIFFORD
CHANCE

CONTACTS

Charles-Henri Laevens
Senior Associate

T +352 485050485
E charleshenri.laevens@cliffordchance.com

Ottavio Covolo
Associate

T +352 485050221
E ottavio.covolo@cliffordchance.com