LOYENS & LOEFF

Brexit: what might change
Data Protection

Introduction

On 23 June 2016 the UK population voted for the UK's exit from the European Union (EU). The applicable exit procedure and certain possible legal consequences of Brexit for Data Protection will be discussed below in the form of a Q&A.

In the short term, we do not identify material changes for the legal practice. The European law and regulations will remain in force until the negotiations between the EU and the UK have been completed and the withdrawal procedure has come to an end. To which extent European law and regulations will also apply following the UK's exit from the EU, will largely depend on the outcome of the negotiations. One of the fundamentals of the EU is the internal market, allowing for the free movement of goods, services, workers and capital (Internal Market). In this context we note that in January 2017, Prime Minister May announced that the UK will opt for a "hard Brexit", meaning that the UK will no longer maintain membership of the Internal Market, nor accede to any associated status. Instead, the UK will seek a free-trade deal with the EU outside the Internal Market.

Brexit – background

Since 2007 (Treaty of Lisbon), the EU Treaty offers a Member State an explicit legal basis to leave the EU (Article 50 TEU). Pursuant to Article 50(2) TEU, the UK can start the exit procedure by giving notice to the European Council. The exit agreement will be concluded on behalf of the EU by the Council[1], acting upon a qualified majority[2] and after having obtained the consent of the European Parliament. The agreement must set out the arrangements for the UK's exit and take account of the framework for the UK's future relationship with the EU. The UK cannot participate in the relevant discussions or decisions of the European Council or Council.

The EU Treaties cease to apply to the UK from the date of entry into force of the exit agreement or, if there is no such agreement, 2 years after the date of notice under Article 50 TEU, unless the European Council, in agreement with the UK, unanimously decides to extend this period. The exit procedure has never been called for and the way forward is full of uncertainties. Apart from Article 50 TEU, no further provisions or guidelines apply.

---

1 The Council consists of a representative of each Member State at ministerial level, who may bind the government of the Member State in question and cast its vote (Article 16 TEU).

2 The qualified majority shall be defined as at least 72 % of the members of the Council representing the participating Member States, comprising at least 65 % of the population of these States (Article 238(3)(b) TFEU).

LOYENS & LOEFF

The current UK Data protection legislation is the result of the implementation of Data protection Directive 95/46/EEC. On 25 May 2016, the EU adopted the General Data Protection Regulation (GDPR) which will become directly applicable in all EU and EEA Member States as from 25 May 2018.

This uniform EU regime sets out higher standards of protection and sanctions in the event of infringements and will become directly applicable without national implementation. Given the timing, the GDPR is likely to enter into force in the UK before Brexit. This has been confirmed by the British government who announced that the UK will be implementing the GDPR. In this case, the UK will have to replace this EU regulation with a new UK data protection law.

Q&A - Data protection

Will the EU General Data Protection Regulation apply post-Brexit?

The future of the UK data protection regime will depend on the outcome of negotiations between the UK and the EU.

(i) Within the EEA

If the UK joins the EEA, the GDPR will remain applicable (through a national implementing act) in the UK. In such a case, Brexit will have a mitigating effect on the data protection regime, which will remain the same as across the EU.

(ii) Outside the EEA

If the UK does not join the EEA, the relationship between the UK and the EU with respect to data protection will have to be organised by agreement and implemented by national law.

Could the UK data protection regime be less stringent than the European regime?

(i) Adequate level of protection

The UK is not likely to implement a disruptive or liberal regime, given the extra-territorial scope of the GDPR and the risk of impeding transfers of data between the EU and the EEA Member States.

Firstly, the new GDPR will in any case still apply to a UK-based company that processes the personal data of EU data subjects where processing is related (1) to the offering of goods or services to individuals in the EU or (2) to the monitoring of their behaviour in the EU.

Secondly, the current Directive as well as the GDPR restrict any transfer of personal data to a third country which is not providing an "adequate" level of protection for personal data.

For these reasons, the UK is likely to adopt a regime which will be considered by the EU Commission and the EU Court of Justice as providing an "adequate" level of protection in order to allow UK businesses to continue to share personal data with the EU and EEA countries.

This has been confirmed by the UK Information Commissioner's Office (the UK Data Protection Authority) which emphasised, in a press release of 1 July 2016, that "With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organisations and to consumers and citizens."

LOYENS & LOEFF

LOYENSLOEFF.COM

(ii) Liberal national regime

If the UK does, however, decide to adopt a liberal national regime, it could opt for a "two-tier system" including one GDPR- level standard of protection for the data transferred from the EU and the EEA, and a more liberal standard designed for domestic data, easily transferable outside the EU and the EEA (and thereby providing a competitive advantage to the UK). It remains to be seen, however, how this scenario could be implemented in practice and whether the EU will still consider this double standard as ensuring sufficient guarantees to provide an adequate level of protection of personal data. Moreover, it is also questionable whether UK citizens would accept a lower level of protection of their personal data.

Will GDPR "one-stop shop" cooperation apply to a UK-based business?

If the UK opts for a national regime (and does not join the EEA), UK-based businesses will inevitably lose the advantage of the "one-stop shop" provided by the GDPR, which foresees the cooperation between one "lead" supervisory authority and the other supervisory authorities concerned by the processing of personal data as involving several EU Member States. In other words, a UK-based business outsourcing its processing activities to an EU Member State will inevitably be regulated by both UK and EU data protection legislation and will also fall under the authority of both UK and EU data protection authorities.

What next?

Once the UK invokes Article 50 TEU, the UK and the EU will negotiate the terms of Brexit. It will be a highly political process and the outcome is as yet unclear. Therefore it is of the utmost importance to monitor the developments and the potential impact on your company's position closely. We will keep you informed about further developments.

Please contact your trusted adviser at Loyens & Loeff or send an e-mail to Brexit@loyensloeff.com if you have any queries.

Impact of Brexit

UK within the EEA	UK outside the EEA	
GDPR remains applicable	UK national regime providing an adequate level of protection	UK national regime not providing an adequate level of protection
Free transfer of data within the EU and EEA	Free transfer of data between the UK and the EU and EEA	No transfer of data between the UK and the EU and the EEA