Brexit and Data Protection

How will Brexit, in whatever form it takes, affect data protection law in the UK?

There are a number of alternative options for the UK's exit as a whole, depending on the outcome of the negotiations, and we don't yet know when we'll have certainty on this question. The main options being discussed are as follows:

1. We stay in the European Union (EU). Until Article 50 of the Lisbon Treaty is triggered, there remains the possibility that the UK will not, in fact, leave the EU at all.
2. We leave the EU, but stay in the European Economic Area (EEA). The EEA is a separate treaty agreement between all the members of the EU plus Iceland, Liechtenstein and Norway. The EEA Agreement requires EEA states to incorporate EU legislation covering the four freedoms (free movement of goods, services, persons and capital) into their domestic law.
3. We leave the EU and the EEA. In terms of trade arrangements, the options here include joining the European Free Trade Area (EFTA) (the Swiss model), negotiating individual trade terms with the EU (the Canadian model), or falling back on World Trade Organisation trade terms.

Whatever the outcome, there is no doubt that businesses should keep preparing for the General Data Protection Regulation (GDPR). The GDPR will continue to apply across the remainder of the EU, and so any organisations operating across the continent will still need to comply. Moreover, any UK businesses which process data about EU nationals (whether as a controller or a processor) will be subject to the GDPR as an overseas controller, in the same way many US companies will be.

The GDPR becomes applicable across the EU on 25 May 2018, which is several months before the earliest that the UK's exit negotiations could be completed – even if Article 50 was triggered tomorrow. In view of this, and the concerns around data transfers, it is highly likely that any UK Act of Parliament concerning data protection would be very similar to the GDPR.

The **table below** explores what each of the options above mean in respect of data protection.

Possible Outcome	Remain in EU	Remain in EEA	Leave the EU and EEA, negotiate alternative trade arrangement or fall-back on WTO trade terms. This leaves (at least) two potential alternatives for the UK's data protection law.	
Options for UK data protection law	**The UK remains subject to the GDPR as initially planned prior to the referendum.** Some commentators are questioning whether Brexit will happen at all. If the UK stays in the EU, the GDPR will become applicable on 25 May 2018, as intended prior to the referendum.	**The UK remains subject to the GDPR, as part of its continuing participation in the EEA and/or single market.** In order to remain part of the EEA, the UK will have to accept the vast majority of EU legislation, including the GDPR. The main distinction from EU membership is that instead of being automatically applicable in the UK, the UK Parliament would need to implement the GDPR into national law. However, the UK would have no flexibility to make any amendments to the text.	**The UK is not part of the EEA, but decides to retain the GDPR wholesale in its national legislation.** Even outside the EEA, the UK could still decide to adopt all of the GDPR into UK law. Since the GDPR will already be applicable by the time the exit negotiations are completed, this would potentially be the simplest solution for the UK post-Brexit. There would be certain sections such as the One-Stop-Shop, the European Data Protection Board and Binding Corporate Rules, which would not work purely as a matter of domestic law, but otherwise the UK could simply continue to apply the majority of the GDPR 'as is' – but as a UK Act of Parliament, not an EU Regulation.	**The UK adopts a new, more business-friendly version of the GDPR ('GDPR-lite')** The UK could decide to base its national law on the GDPR but make certain changes to suit UK businesses. We would expect these to be aimed at making the GDPR more 'business-friendly'.
Processing obligations	As in the GDPR. Obligations on controllers and processors to ensure fair and lawful processing.	Precisely as in the GDPR.	Precisely as in the GDPR.	Based on the GDPR, but some modifications to be more business-friendly.
Transfers of data from the EU to the UK	No data transfer restrictions.	No data transfer restrictions.	Potential data transfer restrictions.	Potential data transfer restrictions.

Commission adequacy finding	Not needed.	Not needed.	UK would almost certainly achieve adequacy status, so no data transfer solution is required.	UK would seek adequacy status, but may not achieve this. 'Adequacy' is increasingly being interpreted to mean 'equivalency', so any deviations from the GDPR would be heavily scrutinised by the Commission. The Commission could also scrutinise other aspects of the UK's legal regime, e.g. government surveillance laws. The planned Investigatory Powers Bill could be very significant in this analysis. If the UK did not achieve adequacy status, alternative data transfer solutions would be needed to transfer data from the EU to the UK. This could be: • Model Clauses • Binding Corporate Rules The UK could negotiate its own 'Privacy Shield' with the EU.
Transfers of data out of the UK to non-EEA countries	Restrictions on transferring data outside the EEA.	Restrictions on transferring data outside the EEA.	Restrictions on transferring data outside the EEA.	Transfer restrictions apply, but likely to be more flexible, e.g. allowing controller to make its own "adequacy" assessment. The UK could also develop its own transfer solutions, such as UK Model Clauses.
Model Clauses	Model Clauses provide adequate safeguards for transfers from the UK. Any decision by the CJEU in respect of Model Clauses applies to the UK.	Model Clauses continue to provide adequate safeguards for transfers from the UK. Any decision by the CJEU in respect of Model Clauses applies to the UK.	Model Clauses continue to provide adequate safeguards for transfers from the UK. The UK could also develop its own Model Clauses.	Model Clauses continue to provide adequate safeguards for transfers from the UK. The UK could also develop its own Model Clauses.
Privacy Shield (if adopted)	UK controllers can use the Privacy Shield for transfers to the US.	UK controllers can use the Privacy Shield for transfers to the US.	Privacy Shield is not available for UK-US transfers.	Privacy Shield is not available for UK-US transfers, but could be used as evidence for a controller's own adequacy assessment.

			Potentially, the UK could seek to negotiate its own agreement with the US (similar to the US-Swiss Safe Harbor arrangement).	Potentially, the UK could seek to negotiate its own agreement with the US (similar to the US-Swiss Safe Harbor arrangement).
Binding Corporate Rules (BCRs)	UK controllers can rely on BCRs. The ICO is part of the review procedure and can grant authorisations as the 'lead' Data Protection Authority (**DPA**).	UK controllers can rely on BCRs. The ICO is still part of the review procedure and may be able to grant authorisations.	UK controllers can rely on BCRs, but the ICO is not formally part of the GDPR review procedure and/or able to grant authorisations. It is possible that an informal mutual recognition procedure is agreed, as is the case now.	UK controllers can rely on BCRs, but the ICO is not formally part of the GDPR review procedure and/or able to grant authorisations. It is possible that an informal mutual recognition procedure is agreed, as is the case now.
One-Stop-Shop (OSS)	OSS will apply, and the ICO will be a UK controller's 'lead' DPA. ICO has full participation rights in the European Data Protection Board.	OSS continues to apply, and the ICO will remain a UK controller's 'lead' DPA. ICO's role on the European Data Protection Board is uncertain.	OSS does not apply. A controller subject to UK and EU law could face separate enforcement action from the ICO and other EU DPAs. However, we expect there would be a degree of co-operation and information-sharing.	OSS does not apply. A controller subject to UK and EU law could face separate enforcement action from the ICO and other EU DPAs. However, we expect there would be a degree of co-operation and information-sharing.
Court of Justice of the European	UK bound by rulings made by the CJEU on the GDPR. UK Courts could make referrals in the event of ambiguity.	UK bound by rulings made by the CJEU on the GDPR. UK Courts could make referrals in the event of ambiguity.	UK not bound by CJEU decisions.	UK not bound by CJEU decisions.