



# Confidential information and trade secrets

In the UK, the common law protects information that has the necessary quality of confidence and is disclosed in circumstances imparting an obligation of confidence. Consequently Brexit should have a limited impact if any.

The Trade Secrets Directive was formally adopted by the Council of the European Union on May 27th 2016 and came into force on July 5th 2016, and the UK has until June 9th 2018 to transpose the Directive into national law. So we can expect this to come into force in the UK before exit, though whether the UK Government will implement the Directive in a narrowed form we cannot yet know. The Directive's purpose is to harmonise EU law on trade secrets, with a broad definition of 'trade secret' as information that is secret, has commercial value because it is secret, and has been subject to reasonable steps by the

person lawfully in control of it to keep it secret. As a result information currently protected by the law of confidentiality in the UK may fall within the scope of this Directive. However, given the UK law today it is unlikely this Directive will make any harmful change to the situation as understood today.

## Data Protection

Leaving the EU will have limited impact on data protection obligations in the UK. If the UK remains in the EEA, as is the expected default position, it will have to implement the forthcoming General Data

Protection Regulation (GDPR) which applies throughout the EEA thereby keeping the UK in line with data protection regulation throughout the EU and there will be no effect on data transfers to/from the UK. Even if the UK does not remain in the EEA, and does not implement the GDPR, UK businesses will be subject to EU regulation if they are offering goods and services to EU citizens and/or monitoring the behaviour of EU citizens. The UK has always been a first mover on Data Protection and pre EU regulation had standards that the EU has since adopted and so in all scenarios it is expected the Data standards will remain sufficient to enable EU wide compliance and keep the UK as a leader in Data matters.

So if the UK ends up leaving the EEA it is not believed to be difficult for the necessary safeguards to be employed when sending data to the UK from the EEA or vice versa to satisfy EU and Member State Regulators. There has been a suggestion that the UK



may need to implement a system similar to that in place for data transfers to the US (the Privacy Shield II), even if the new EU regulation is adopted, because of concerns regarding mass surveillance by the government and proposals to extend investigatory powers. This is a self-certification system for companies to declare that their data protection systems are adequate in terms of EU requirements. Though again as the UK is closer to the EU approach to Government surveillance rules than say the USA, it is not expected to be an issue, and the UK will have a system that the EU can accept as compliant, especially as the UK's data regulator is one of the most respected in Europe.

Alternatively, the UK could become a country registered with the EU (as is the case in Jersey, Israel, New Zealand for example) as having a positive finding of adequacy. Such countries have been approved as having sufficient protection for personal

“

**There has been a suggestion that the UK may need to implement a system similar to that in place for data transfers to the US, even if the new EU regulation is adopted, because of concerns regarding mass surveillance by the government and proposals to extend investigatory powers.**

”

data so that European businesses can send data to them without putting further safeguards in place. A positive finding of adequacy may depend on the UK adopting the GDPR, but the UK is unlikely to have any problem matching its requirements.

Finally, UK businesses will still have available to them Model Clauses (for data transfers between entities, whether or not they are connected) and Binding Corporate Rules (for use by businesses with connected entities in multiple jurisdictions) which

enable those outside the EEA to send personal data to and from the EEA.



**James Tumbridge**  
jtumbridge@vennershipley.co.uk