# Ringfence™: Brexit, GDPR & Privacy Shield

*If you thought that Brexit meant that you didn't have to comply with new EU General Data Protection Regulation (GDPR) you might want to think again….*

- Any UK company which trades in the EU will still have to comply with EU GDPR regardless
- It looks increasingly likely that the UK will need to upgrade its data protection laws to be consistent with EU GDPR as part of Brexit
- Moving outside of the EU also affects UK/US data transfers and safeguards, again it is likely that EU/US Privacy Shield (Safe Harbour replacement) consistency will be required
- With Brexit likely to take until 2019 at the earliest UK organisations will still need to consider compliance with EU GDPR since it will come into effect 25 May 2018

## GDPR

The new EU General Data Protection Regulation was finally approved by the European Parliament in April 2016 and must be formally in place across all EU member states by May 2018. These significantly raise the bar on data protection and privacy, effectively setting the global standard in terms of protecting individuals' fundamental privacy rights.

- Introduces potential fines of up to 4% of global turnover or €20M for significant data breaches
- Extends the definition of personal data to include genetic, mental, cultural, economic or social information
- Stronger, explicit consent model for collecting personal data – can no longer rely upon implicit consent and have to respond to changes in consent (e.g. "opting out")
- Public authorities processing personal information and some other organisations processing thousands of items of personal data must appoint a Data Protection Officer (DPO) – regardless of size
- Requires mandatory privacy impact assessments (PIAs) to be built into projects to minimise risk to data subjects
- Requires significant data breaches to be notified to local data protection authority (the ICO in the UK) within 72 hours of discovery
- Introduces the "right to be forgotten", strengthening the requirement not to hold personal data longer than absolutely necessary or use it for other purposes, also to delete data if requested by the data subject

- Extends liability beyond data controllers to all organisations that process personal data on their behalf (although data controllers still have overall accountability & responsibility)

- Requires “privacy by design” for software, systems and processes to ensure compliance with the EU GDPR principles of data protection and privacy

- Allows any EU data protection authority to take action against organisations regardless of where the company is based

## EU/US Privacy Shield

This was approved in July 2016 and replaces the now defunct EU/US Safe Harbour agreement for data flows of personal data between the US and EU.

- Fully consistent with EU GDPR, puts more onus on companies transferring information between EU/US and makes them more accountable for any data breaches

- Further restricts US government access to personal data for EU citizens on US computers and safeguards against “mass surveillance”

- Provides enhanced data subject rights, stronger recourse and enforcement – also separate rules for transferring human resources data to maintain compliance with EU labour laws

## Options & Opportunities

*You could choose to “wait and see” what happens in terms of Brexit and the future UK data protection and privacy framework - however this is a potentially risky strategy given that EU GDPR looks like it will still come into effect in May 2018 in the UK, also that the smart money is increasingly on the UK aligning itself to both the EU GDPR and EU/US Privacy Shield agreements.*

*UK based organisations aligning themselves to the EU GDPR sooner rather than later are likely to be better positioned competitively, as well as being at lesser risk of cyber-crime or data breaches.*

*At the very least it would be prudent to review what personal data you currently collect and use, where it is held and who is involved in processing it - the simplest solution might well be to repatriate any personal data within the UK sovereign jurisdiction until the UK has left the EU and the data privacy requirements and legislation have settled down again.*


### Contact us

info@ringfence.solutions | +44(0)113 320 0407 | www.ringfence.solutions