DATA PROTECTION AND ECOMMERCE

A Report commissioned by City, University of London, Industrial Strategy Seed Fund. February 2018

Introduction

Creative sector companies are likely to be significantly impacted by data protection laws particularly given the fact that they are likely to store, analyse and transfer personal data as part of their day to day operations.

This review looks at two general areas that will impact companies

i) The new General Data Protection Regulation ('GDPR') – the largest overall change in data protection laws in 20 years. This is on most international companies' agenda's particularly given the large fines that will accompany it; and

ii) Data transfers – the restrictions regarding data transfers inside and outside the EU – which may particularly be complicated post-Brexit. This specific restriction (which applied under previous laws as well as GDPR) creates complexities to global companies and could potentially be further complicated as a result of Brexit.

1. General Data Protection Regulation ('GDPR')

One of the reasons that GDPR impacts UK companies even after Brexit is that it affects all companies that are trading with or processing personal data of EU individuals. Under the GDPR, the definition of personal data is set out in Article 4 as:

an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location number, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

As such, the definition of personal data is so broad under EU law that it encompasses any information that could potentially identify an individual. Obviously, this could include a name, or email address, or even more transcient information such as IP addresses.

Moreover, extraterritorial reach under Article 3 of the GDPR means that it will impact all global and US multinationals, i.e, any company that will be processing data of individuals within the Union could be impacted.

1.1 GDPR – what changes?

Some of the key changes under GDPR are as follows:

- Increased fines: While there are some changes to existing laws under GDPR, one of the key reasons that companies are paying attention to the rule changes is quite simply the level of potential fines – the greater of 4% of global turnover and 20 Million Euros. For large multinationals and technology sector companies, this is significant.

- Greater governance: Another issue that companies face is the governance requirements – have they a proper GDPR governance team in place. This is required to ensure that internal privacy impact assessments are carried out, responding to subject requests (access requests, deletion requests, correction requests etc), or managing any incidents such as data breaches. In relation to data breaches, companies will also need to ensure they adhere to good industry security practices – which could for instance include a third party attestation (SOC2 or ISO27001).

- Stricter contractual commitments: Finally, under GDPR Article 28(3), companies will need to adhere to explicit contractual commitments – around processing data, audit, and giving individuals' rights, so these will require updates to terms and conditions for all customer contracts. Frequently, this will be in the form of a 'data protection addendum'.

All of these changes will bring with them a greater compliance and administrative burden on EU creative companies processing personal data.

2. Data Transfers

One specific area of data protection (including under GDPR) that is likely to create the most confusion is that of data transfers – particularly when the alignment of the UK legal regimes to that of the EU is uncertain.

While the UK regulator, the Information Commissioner's Office, has publicly stated the UK will implement GDPR[1], one of the challenges UK companies will face post Brexit is the fact that, even if implemented, the EU may not view this implementation as aligned with their requirements. The key mechanisms to enable data transfers between the EU and third party countries include:

- Adequacy finding – note that only 10[2] countries, as well as Canada (Partial) and the US (Safe Harbor, now Privacy Shield), have received such a finding and it takes extensive review and negotiation with the European Commission.
- Model clauses – this undoubtedly increases the administrative burden on UK companies. Also, the validity of model clauses may be for dispute.
- Binding Corporate Rules – a set of fully approved internal privacy rules which need to be officially approved. This process is likely to be out of reach for most creative SME's.

The below graphic suggested by Eduardo Ustaran of Hogan Lovells, suggests the probable solutions for UK companies.

[1] https://iconewsblog.org.uk/2016/10/31/how-the-ico-will-be-supporting-the-implementation-of-the-gdpr/
[2] This list currently comprises: Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay. An uptodate list is available from the European Commission website.

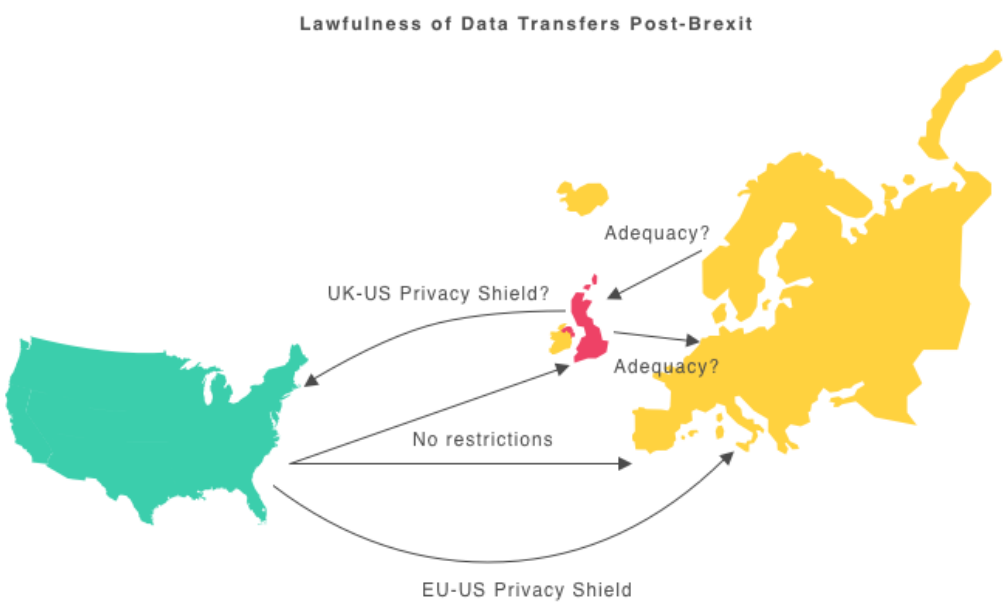

Figure 1 Data transfer solutions post Brexit

While there are likely to be solutions to the issue of data transfers for EU creative companies post Brexit, the administrative hurdles, uncertainty and costs will undoubtedly increase, and more pertinently, doing business with EU customers will be more difficult.

However, data transfers is only one of the challenges Creative sector companies will face. On the basis that the UK implements GDPR in full, this will have wide ranging ramifications far beyond simply data transfers and these are described further below.

3. General Privacy Awareness

In order to assess the existing approach taken by companies in dealing with issues such as GDPR or data transfers, we contacted multiple cloud vendors to assess their responses and awareness of privacy laws, their privacy governance and IT security posture.

Our overall assessment was that almost half of the 46 companies reviewed were struggling to meet their privacy compliance obligations. We note that this was based on a brief email exchange whereby many were unable to answer basic questions to satisfy compliance.

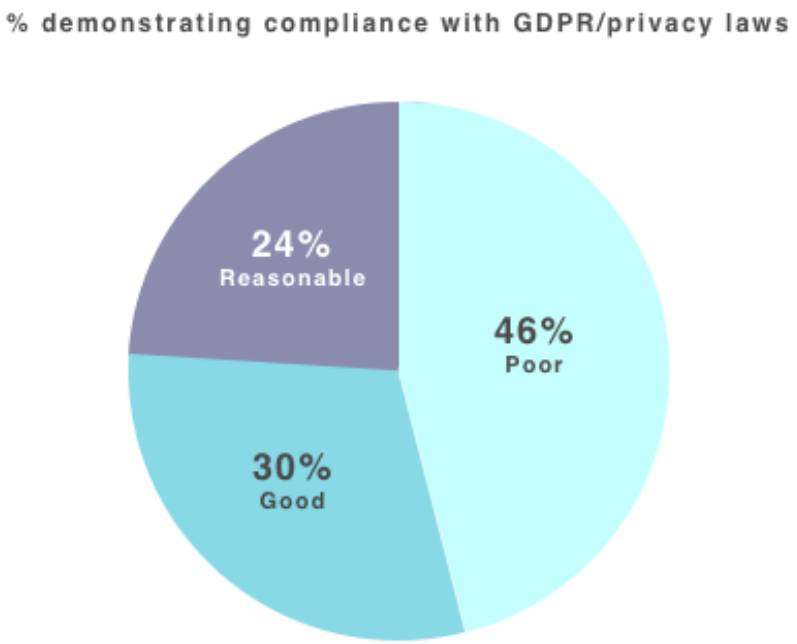

Figure 2 Assessment of privacy/GDPR readiness across a selection of companies.

Additionally, less than a third of companies contacted could provide confirmation of mature privacy compliance including governance and appointment of a data protection officer.

A reasonable number of companies had information security attestations such as ISO27001 or SOC2 and privacy shield attestation.

4 Conclusion

Privacy and Data Protection law will present a significant hurdle to creative sector companies and are likely to involve an increase in overheads and administration in handling the complexities as a result of data transfer obligations post-Brexit and the new GDPR.

However, most of the issues that may be encountered will likely have clear legal solutions to minimize risks of non-compliance, and for companies that have the resources to spend on ensuring compliance with best practices, the complexities are likely to lead to new opportunities and increased competitive advantages.