Brexit Toolkit: UK Creative Industries and the Data Economy in a Post-Brexit Britain

2020

Responsible Marketing

DMA
Data & Marketing Association

Contents

Introduction

The UK Creative Industries as global leaders

The UK's exit from the European Union poses significant risks and opportunities for the UK's creative industries. To maintain global leadership status, we must make sure that the creative industries remain vibrant and dynamic after Brexit .

British creativity does not just secure jobs and economic prosperity at home, it also supports British 'soft power' all over the world.

This solidifies our ability to collaborate with countries all over the world and help to shape international perceptions of the UK.

The Data Economy and the Creative Industries

Cross-border data flows are the veins that feed the modern global economy. The success of data-reliant sectors – such as advanced manufacturing, logistics, financial services, data-analytics, marketing, and IT – are contingent on the UK's ability to maintain data-flows with the EU.

The UK is an international leader for data flows, which have increased 28 times between 2005 and 2015. The UK currently has the largest data centre market in Europe, worth over £73 billion, with over 75% of UK data transfers occurring within EU countries.

The EU knows this is an important issue. Estimates suggest that around 43% of all large EU digital companies were started in the UK, and the UK's position on the EDPB has driven a lot of pan-European legislation implemented today.

The Creative Industries employ around 3 million people in all (9.3% of the UK total) and contributed £87.4bn to the UK's economy in 2015. They account for 9.4% of all services exported from the UK, worth £21.2bn, with 45% going to the EU; and for 5.2% of all goods' exports, another £14.7 billion in 2015.

The UK has the largest internet economy of any G20 nation at over 10% of GDP. Nesta estimates that digital technology contributes £160 billion to the UK economy and 1.56 million jobs with 12% of them in data management and analytics solutions.

For the economy to thrive post-Brexit, the UK must remain a global centre of excellence for digital transformation, data analytics, data security and innovation.

Data and Marketing

The free flow of data

Data drives economic growth in the creative industries, allowing for intelligent insights into consumer behaviour and, ultimately, a tailored and personal offering from brands.

UK creative businesses operate across Europe and rely on the supply of data to inform and facilitate their work. Cross border exchanges of personal data are therefore paramount. Brexit will affect the organisations' ability to send personal data from the EU to the UK.

As a member of the EU, organisations based in the EU were able to freely send personal data between the UK and EU. The UK Government, in recognition of UK's alignment with the EU on data protection, will permit the transfer of data from the UK to the EU after Brexit.

However, the EU cannot make the same offer until the UK reaches 'third country status' (which it did in January 2020) and has deemed that the UK's data protection practices are sufficiently protective to merit 'adequacy status'.

Adequacy status is a measure in the General Data Protection Regulation (GDPR), which allows the EU Commission to certify that a country has adequate levels of data protection. Once certified, EU member states can exchange personal data with that country.

The EU and UK began adequacy discussions in June 2020.

Previously, the European Commission has recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan. Adequacy talks are ongoing with South Korea.

The UK Government argues that the UK's unique position of regulatory alignment with the EU means the adequacy process should be relatively straightforward.

Indeed, it is claimed that the UK and EU are now treating the adequacy talks as a technical agreement to be reached rather than a political one, which means reaching this agreement will not be contingent on any political to-and-fro that could usurp other aspects of the post-Brexit deal.

However, the charge has often been levied that the UK's security service data gathering for surveillance purposes breaches EU human rights law. This was contested however as, while it was a member of the EU, the UK's security practices were contributing to EU security and therefore were protected. Similarly, specific judgements had not been issued that banned data gathering for surveillance purposes.

That was until 6 October 2020, when the European Court of Justice ruled that EU countries cannot retain citizens' data in a sustained way for intelligence purposes (unless there is a clear and present danger to national security).

This could be a huge blow for the UK's hope of securing a data adequacy deal with the EU. If data from an EU citizen gets sent to the UK, the UK's surveillance services will be able to retain it for surveillance purposes, which the EU has decreed is a breach of human rights. So, if there is a risk that an adequacy agreement could allow the UK to breach EU citizens' rights, the EU Commission is obligated to prevent the agreement to protect those rights.

Furthermore, at a House of Commons Digital, Culture, Media and Sport Committee hearing on 13 October 2020, Dr Jiahong Chen, a Research Fellow in IT Law at Horizon Digital Economy Research at the University of Nottingham, outlined that the Investigatory Powers Act (2018) posed similar problems for data adequacy.

He, and many other academics, argue that the Investigatory Powers Act allows the UK Government to gather and keep personal information on individuals for the purposes of decision making in visa applications. After the EUCJ ruling, this kind of data gathering would also be illegal in the EU.

On top of this, the UK Government's running down the clock on negotiations means a no-deal Brexit is not unlikely.

While adequacy is being treated as a separate technical issue, in the case of a no-deal Brexit, there would be less impetus to secure an agreement on data protection. Therefore, without alternative arrangements, the processing of personal data of EU citizens in the UK would become illegal.

While an adequacy agreement would be however, there are some solutions to this which we will discuss in the next section.

How to Exchange personal data with the EU

Data Adequacy

As noted, a data adequacy agreement is by far the best solution for the transfer of data between the EU and UK post-Brexit. For this to happen, the EU would determine that the UK's data protection standards and respect of human rights was essentially equivalent to the EU's practices.

In this case, companies in the UK would be permitted to access, process, and store the data of EU citizens in the UK.

The UK has, in essence, made the EU adequate in the eyes of UK law, having legally recognised all EEA states, EU and EEA institutions, and Gibraltar as providing an adequate level of protection for personal data.

Where the EU has made an adequacy decision in respect of a country or territory outside of the EU prior to exit day, the UK Government intends to preserve the effect of these decisions on a transitional basis.

However, those countries could require similar examination of UK data protection standards to reciprocate such an agreement.

If adequacy is reached the only other development for EU organisations will be obligations that arise because of the UK Government intending to replicate Article 27 of the EU GDPR.

This requires a controller or processor not established in the EEA to designate a representative within the EEA. The UK will require controllers based outside of the UK to appoint a representative in the UK.

Data adequacy negotiations will carry on until an agreement is reached, or not. If a data adequacy agreement has been reached businesses will be able to carry on as they do now.

Standard Contractual Clauses (SCCs)

In the absence of adequacy decision between the EU and a third country, an adequate level of data protection can be ensured by other mechanisms such as SCC.

If the EU company wishing to transfer data to a third country concludes the SCC with the company in the third country which is to process the personal data.

SCCs are legal contracts which can be signed by the organisation processing personal data and the person or organisation having data processed.

These are – as the name implies – standardised and downloadable from the EU Commission website. When both parties agree for these to be used, the data transfer can be completed using the same process as if there were open data flows.

While a relatively straightforward solution, an SCC must be used for every data transfer. This may make implementation cumbersome and resource heavy. While larger organisations may have the manpower to implement this, smaller organisations may struggle to cope with the administrative burden.

SCCs are the next best solution to replicating the free-flow of data in the case of a no-deal Brexit, or a Brexit deal that does not include a data adequacy agreement.

Through the recent Schrems II case the ECJ confirmed the SCCs to be valid. This validation of the use of SCCs meant businesses can be confident about using them if no adequacy agreement is reached with the EU.

Nonetheless, SCCs have been validated because they offer extra protections for EU-origin data going into jurisdictions where the data may be subject to other processing based on laws in the receiving jurisdiction.

Specifically, SCCs make provisions for the cancellation of the contract and rejection of data transfer if the person or organisation sending EU-origin data is not happy with the potential gathering of the data for additional purposes (chiefly security purposes) in the receiving jurisdiction.

If both parties are aware of all potential additional data gathering but still agree to implement the SCC, they may proceed with the data transfer.

SCCs are not common on a mass scale yet, but already some concerns have been raised about the administration and time required to implement SCCs. An SCC is required for every data transfer adding in bureaucracy to the mix, and organisations in other jurisdictions are often not aware of their existence, let alone their purpose.

So, while this is the next-best solution after data adequacy, it will likely still be greatly damaging to organisations' ability to transfer data.

Codes of practice

A useful tool made available through the GDPR is the creation of industry codes to detail good practice which adheres with EU data protection laws.

When organisations sign up to this code and pass a compliance test, this would confirm that they work in-line with EU data protection practices and can freely process the data of EU citizens, continuing to do business with the EU on the same basis as they do currently. In other words, this would essentially be an industry-specific adequacy agreement.

Together with our European partner body, FEDMA, the DMA is in the process of writing one of these industry codes. This would offer a sanctuary for our industry and for any business that wishes to continue to trade with the EU on the same terms which exist today.

Both EU partners and the Department for Digital, Culture, Media and Sport have issued their support for the DMA and FEDMA's efforts, and have said they will do what they can to speed up the process and support in any way.

It is unclear how long it will take to get the code approved, but the DMA is confident the interested parties (including those on the EU side) are keen to get this approved as soon as is practically possible.

Similarly, when the code is approved, companies will need to be assessed and cleared through the compliance process before they can operate freely under the guidelines.

The time it would take to achieve compliance is unclear, though proactive companies with strong data protection practices will obviously complete the process speedily. While this option is not on the cards at present, it is the ideal method of conforming to EU practices in the case of no-deal Brexit, or an insufficient deal.

Even in the case of an adequacy agreement, conforming to the FEDMA code will be a validation of data protection practices and will offer assurance that your organisation is complying with the law.

Check into the DMA website for updates and further information.

Binding Corporate Rules (BCCs)

In short, BCRs allow businesses to have their data protection practices validated by the EDPB, which would allow them to process the personal data of EU citizens on the same basis which currently exists.

To create a BCR, the company must draw up their business practices in conformity to EU law and submit them for approval. This is resource heavy and would require significant drafting. Equally, the approval timeline is lengthy.

This means that if a business has not already started the process, this would not be a viable option as the earlies they could receive approval would be 2021. Furthermore, a European regulator, like the Information Commissioner's Office, must approve it.

Organisations that have their BCR approved by the UK Information Commissioner's Office ('ICO') as their BCR Lead Supervisory Authority (LSA) need to identify a new BCR LSA in the EU, and must amend their BCRs before the end of the Brexit transition period.

Organisations with BCRs already approved but with the LSA located in an EU country will have to obtain a new approval decision from the EDPB.

If the changes are not obtained by the end of the transition period (31 December 2020), organisations formerly with BCRs will not be able to rely on them to transfer EU-origin to the UK.

Brexit and UK-USA Data Transfers

In 2016 the EU and USA agreed a 'privacy shield' agreement, which allowed the transfer of data between the two jurisdictions.

This agreement, however, was struck down by the European Court of Justice in the 'Schrems II' case (Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems), as it was deemed EU citizens' data was subject to the US Government's surveillance practices, which went against EU law.

This was because, under US law, companies are obliged to provide the personal data to US authorities as part of their monitoring programs.

Importantly, in that ruling, the EUCJ ruled that Standard Contractual Clauses (SCCs) could be used as legal grounds for data transfers as, in spite of security concerns, they provide certain data protections between the US-based company and EU citizen.

As noted above, the US company would be obligated to find out whether there is the potential for the security services to capture the data from the EU for surveillance purposes. If the data transfer under an SCC means the person's data could be subject to surveillance by the USA, the person with the EU-based data has the right to refuse the SCC transfer.

This is both good and bad for the UK.

First, it tells us that the EU is serious about concerns with third countries' surveillance practices. Given their similarity to the US, it is likely that the UK's surveillance practices will not sit well with the EU Commission as it discusses data adequacy.

However, it also legitimises SCCs as mechanisms for transferring data meaning, whatever happens, these tools can be used in place of an adequacy agreement (with stipulations regarding surveillance as above)

There is also the issue of data transfers between the UK and USA to be examined, however.

Currently, the UK transfers data to the US in the same way as the EU and US (through use of SCCs and, in limited circumstances, derogations set out in Article 49 GDPR). After the UK leaves the EU, however, it will depend on whether the UK has reached a data adequacy deal with the EU as to the type of agreement the UK can or will make with the USA.

Assuming the UK wants data adequacy at all (even if it cannot obtain an agreement right now), it will need to reach an agreement with the US that maintains EU standards of data privacy to protect EU citizens from any UK or USA surveillance data gathering.

Nonetheless, the UK and USA's security agreements and practices are under intense scrutiny, and it will be up to the EU to decide whether these practices contravene EU law or not.

Further Guidance

The UK Government, Regulators and other bodies have provided guidance on the topics discussed in this toolkit. See below for external links:

- UK Government guidance
- ICO guidance
- European Data Protection Supervisor guidance
- European Data Protection Board guidance
- Data Protection Network guidance

Conclusion

While Brexit in any form poses challenges to the UK data, marketing, and wider creative industries, the UK has the chance to create opportunity from Brexit and make sure that the UK's creative industries remain a global leader.

As discussed above, the key issues involve the free flow of data, and industry access to talent.

Uncertainty over the future of these two points could potentially threaten the global status of the UK's creative industries. The best way to prepare your business for the multitude of potential outcomes is to engage in comprehensive planning.

To help our members prepare for Brexit, the DMA continues to work with Governments, Parliaments, and civil service departments in Brussels, Westminster and Holyrood, as well as with industry partners.

For further developments and analysis, keep checking in on the DMA website.

For questions or more specific advice, please get in contact with members of the DMA's policy, external affairs, and legal teams. You can find their details below.

Key Contacts

Should you have any queries or need further support, please contact:

Michael Sturrock
Head of Public Affairs
Michael.Sturrock@dma.org.uk

Asli Yildiz
Head of Legal
Asli.Yildiz@dma.org.uk

John Mitchison
Director of Policy and Compliance
John.Mitchison@dma.org.uk

Mike Lordan
Director of External Affairs
Mike.Lordan@dma.org.uk

About the Responsible Marketing Campaign

Working responsibly means putting your customer-first at each and every touchpoint, in each and every interaction.

It is inherent to how the DMA works – and how we encourage the UK's data and marketing community to work.

That means growing an appreciation of, adhering to and ultimately implementing best practice in marketing approaches, especially in light of the arrival GDPR.

These changes to the governance of data have far-reaching consequences for your business, and are still making waves.

At the DMA we aim to demystify this new regulatory environment so you and your customers can benefit.

Access our GDPR guidance series - developed in accordance with the ICO - to help you on your journey to GDPR compliance.

Our suite of best practice guides tackles a range of key marketing challenges, and are infused with the real-world knowledge of experts and leaders from around the UK data and marketing industry.

The DMA's events calendar is packed with legal update sessions, morning briefings and webinars that harness the expertise of our Public Affairs, Legal and Compliance teams.

Through our world-renowned Institute (IDM) we offer on and offline learning across responsible marketing themes, at individual and corporate levels.

And through learning initiatives run by DMA Talent we ensure the next generation of marketing leaders emerge into the industry fully aware of how to work with a genuine customer-first ethos.

Responsible marketing is in everything we do well.

Head to our campaign hub to learn more, and get involved.

About the DMA

The Data & Marketing Association (DMA) comprises the DMA, Institute of Data & Marketing (IDM) and DMA Talent.

We seek to guide and inspire industry leaders; to advance careers; and to nurture the next generation of aspiring marketers.

We champion the way things should be done, through a rich fusion of technology, diverse talent, creativity, insight – underpinned by our customer-focused principles.

We set the standards marketers must meet in order to thrive, representing over 1,000 members drawn from the UK's data and marketing landscape.

By working responsibly, sustainably and creatively, together we will drive the data and marketing industry forward to meet the needs of people today and tomorrow.

www.dma.org.uk

Copyright and Disclaimer