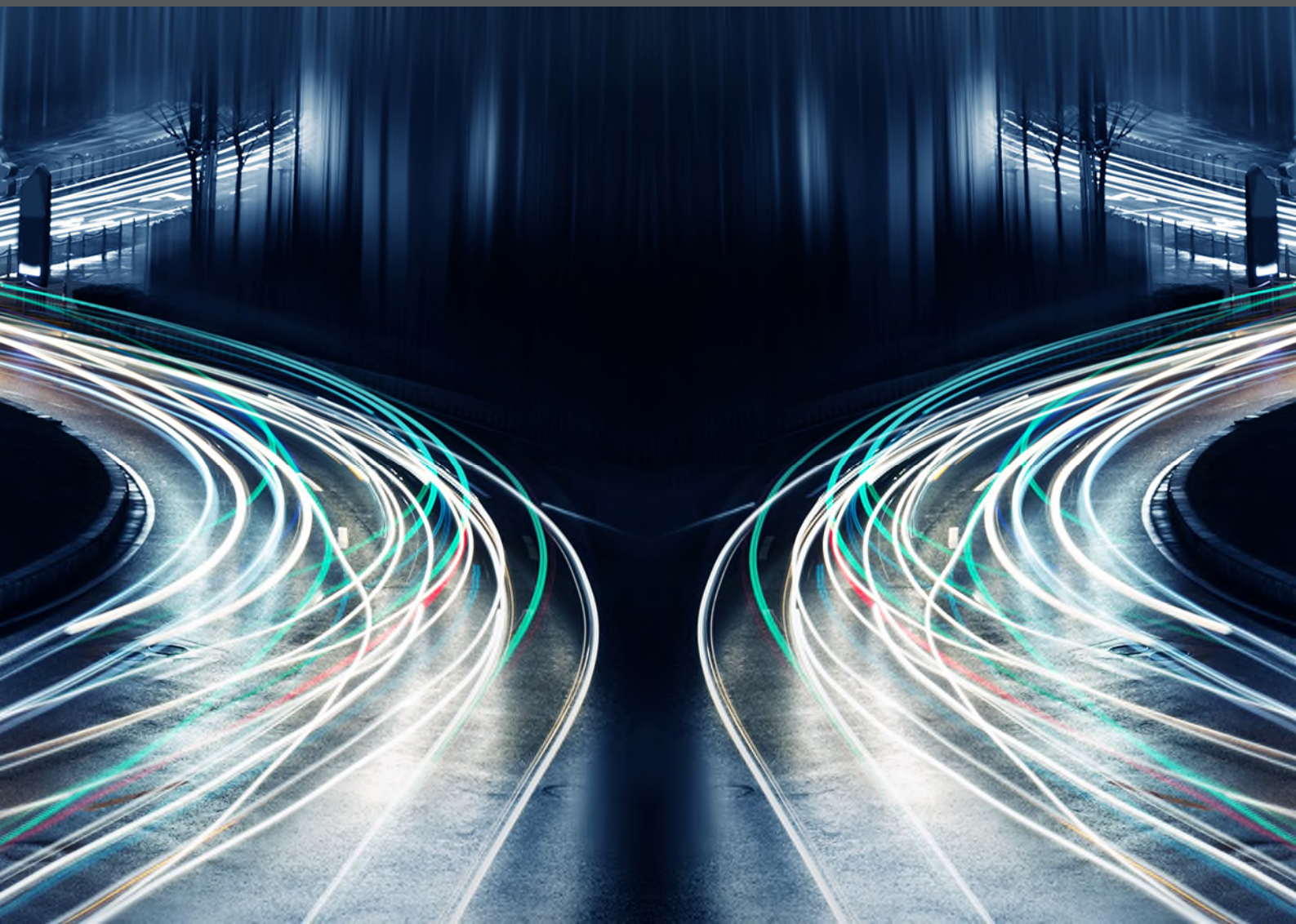
ADDLESHAW GODDARD

BREXIT – PRIVACY IMPLICATIONS

Will Brexit bring an end to the free movement of data?



3 KEY DATA PRIVACY QUESTIONS

By TONI VITALE & RHODA ELISE BRYANS

1. Will it be possible for multinational companies with offices across Europe to operate a single process of collecting and processing personal data?

If the UK chooses to diverge its data protection laws from the new General Data Protection Regulation (GDPR) it will become more difficult to export data to and from the EU and UK (without putting in place EU model clause contracts or binding corporate rules). Implementing model clause agreements between every legal entity in a complex corporate structure is at the very least an administrative headache.

Introducing Binding Corporate Rules is even more difficult, costly, and time consuming (to date only 82 organisations have successfully done so throughout the EU). There is no precedent for a company based outside the EU (as the UK would be post Brexit) based in a country which is deemed not to have adequate protection of data subjects (as the UK might be considered) to successfully implement Binding Corporate Rules and have these approved by EU privacy regulators. So even if a company wanted to roll out rules which adhered to the higher GDPR standards (assuming UK laws do not prohibit this) this may not help.

2. Would the UK be regarded by the EU Commission as a 'safe third country' so that personal data could be transferred to and from the UK?

There is a risk that the UK would not be regarded as a safe third country by the EU Commission (one which had 'adequate protection' of citizens' rights). This would be more likely if the UK decided not to implement the GDPR into UK law. Companies operating in the EU would need to revise the methods they use to transfer data to the UK (such as implementing model clauses or Binding Corporate Rules).

3. Would the UK implement legislation reflecting the new General Data Protection Regulation or would the UK keep the existing Data Protection Act 1998?

The UK government opposed some of the more 'anti-business' aspects of the new GDPR but it may be impossible to ignore entirely. To do so, would run the risk of a finding of 'inadequacy' potentially halting (or making more difficult) the transfer of personal data to and from the EU.

It is possible that the UK would adopt an hybrid position keeping parts of the 1998 Act and adopting some of the new provisions of the GDPR. It is unlikely that data protection will be regarded as a priority subject to be dealt with urgently and in the meantime the uncertainty will pose significant compliance challenges for multinational businesses.

BREXIT: ANALYSIS

The right to privacy is a highly developed area of law in Europe. EU data protection derives from Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Directive). The Data Protection Act 1998 (DPA 1998) gives effect to this Directive. All EU Member States are also bound by the European Convention on Human Rights (ECHR), which guarantees the right to respect for private and family life, home and correspondence in Article 8 of the European Convention on Human Rights.

A UK withdrawal would have a minimal impact in some areas, for example, where individual Member States generally have their own laws, however with data protection, the consequences of a UK withdrawal could be more complicated as the legal landscape is mapped out at an EU level.

Our assessment of the risk level to businesses operating in Europe is somewhere between **moderate** and **high**.

UK businesses operating in Europe will need to reconsider their internal data transfers, terms of business, online operations and the territorial application of privacy laws. Organisations will also need to assess whether to commence or delay their compliance projects for the GDPR, as they may or may not turn out to be necessary

International Transfers of Data

If the UK were to leave the EU, the Data Protection Act 1998 (and its counterparts in other European Member States) prohibit transfers of personal data to countries outside the European Economic Area (EEA), unless they have been recognised by the European Commission as providing "adequate protection" to personal data.

It is not clear whether the UK would become a member of the EEA if it left the EU. If it did not, it would no longer be an automatically "safe" destination for EU personal data. It would have to be approved as providing adequate protection for personal data by the European Commission (Commission). Until that happened, companies based in the EU would need to consider whether they could legitimately transfer personal data to the UK.

Whilst one might reasonably expect that the UK would be approved as providing adequate protection given that the DPA 1998 is based on the Directive, it is not certain. The Commission has reportedly written to the UK Government in the past criticising it for not implementing the Directive fully and international data transfers are a politically sensitive issue within the EU in the post-Snowden era. It is possible that the activities of GCHQ and other security services in the UK might lead the EU Commission to require additional safeguards to protect the rights of UK citizens against intrusive and mass surveillance to be implemented before an "adequacy" ruling would be given.

There are however a number of other approved mechanisms for lawfully transferring data, in particular standard form or 'model' contracts, but they add an additional administrative layer. In some Member States, such as Spain, organisations would also have to obtain prior authorisation from the local supervisory authority before making any such transfer. It is clear therefore that exit could cause some initial disruption to businesses' European operations around data transfers to the UK.

Extra-territorial effect

The current data protection legislation has extra-territorial jurisdiction built into it. By way of example, if a company makes use of a means of processing in the EU (i.e. equipment or a processor located in the EU) to monitor the behaviour or collect personal data relating to an EU citizen, they would be caught by the Directive regardless of where the company is based. Under the GDPR, the test set out in the Directive will fall away, and will be replaced by a more stringent test; if any entity is established outside the EU, and it either (i) offers goods to EU residents; or (ii) monitors the behaviour of EU residents, that entity will be subject to the GDPR. Therefore although coming out of the EU will have some impact, it is not the case that EU privacy law will no longer apply to company's business operations even if they are based outside of the EU.

Brexit would also likely impact on the corporate structuring of international businesses operations. Multinational corporations, for example, frequently look to set up a European hub or data centre for processing data from all their European offices, as a means of avoiding having to deal with EU data transfer restrictions. Ireland and the UK are popular locations for such hubs due to the pragmatic, less process-oriented approach taken by their regulators. If the UK were no longer part of the EU or the EEA, it would no longer be able to benefit from this (unless or until such time as it received the EU's approval as providing adequate protection).

General Data Protection Regulation

If the UK left the EU, the GDPR would no longer be part of the legal framework in the UK (after the transition to implementing Brexit takes place). The current UK government has opposed many of the changes which the Regulation will introduce, which raises the possibility that it may simply maintain the existing UK law, which could be seen as a business-friendly move.

However, there is scope for a high degree of confusion in this sphere, as the GDPR would apply in the UK in the aftermath of a Brexit vote, but before implementation of that exit from the EU and then falls away.

Key question: Would the UK still go ahead to implement elements of the GDPR?

This would be a decision for the UK Government to make. It would also depend on what kind of Brexit the UK decides on and whether to align certain laws with those of Europe. It is highly likely that the Data Protection Act 1998 would still remain in force. It is enshrined within the UK legal system so there would be no change unless the UK decided to make changes to it. The Government might decide in light of a successful 'leave' vote to adopt some parts of the GDPR and imbed these into the DPA by way of an amendment with the goal of bringing UK law into line with Europe. There would however be political sensitivities with this.

Enforcement headaches

In the EU under the GDPR, businesses have the potential to be fined the greater of €20m or 4% of annual turnover for data breaches. Under the EU Data Protection Directive enforcement and fines vary between member states. In the UK the current maximum fine is £500,000. If a data breach occurred solely in the UK then only UK enforcement would follow.

However the position will change if a UK based company commits a data breach which affects European citizen's data held on European servers. This is where the position will become more complicated and a European Supervisory Authority from a member state could potentially take action and impose greater fines.

Would UK citizens lose the 'right to be forgotten'?

At present, the right to be forgotten has been rolled out across Europe by Google and includes google.com (following the *CJEU Case of Google v Gonzalez*).

After Brexit the CJEU decision may no longer apply to the UK and it is possible Google would be permitted to carve out all google.co.uk domains from this blanket shield and UK citizens will lose this right.

A UK Privacy Shield?

In February 2016 the European Commission announced agreement of a new framework for transatlantic data flows. The EU-US Privacy Shield reflects the European Court of Justice (ECJ) ruling of 6 October 2015, which invalidated the old Safe Harbour regime. Agreement is required by all 28 Member states on the new EU-US Privacy Shield. The Privacy Shield is meant to replace an earlier data transfer pact called Safe Harbour. Safe Harbour was invalidated by a court decision in October 2015 (*Maximillian Schrems v Data Protection Commissioner*).

In April 2016 the Article 29 Data Protection Working Party (an EU privacy group set up by the EU Commission) said it was still concerned about the possibility of "massive and indiscriminate" bulk collection of EU citizens' data by the US authorities. The group urged the US and European Commission to revise and clarify several points in the proposed Privacy Shield agreement in order to safeguard EU citizens' personal information. It added that it wanted further guarantees about the powers a US official would have to handle complaints from EU citizens.

Whilst the EU-US Privacy Shield has gone back to the drawing board, the key question is would the UK require its own version of the Privacy Shield to ensure the EU Commission provides the UK with a finding of "adequacy" which would make cross border data flows easier to implement?

These are the key terms of the Privacy Shield that the UK would probably have to consent to:

- An ombudsman to handle complaints from EU citizens about the UK security services spying on their data
- UK Security services / the Home Office to give written commitments that Europeans' personal data will not be subject to mass surveillance
- The UK to agree to an annual review or audit to check the new system is working properly

Conclusion: breaking free of red tape or bureaucratic nadir?

Brexit will have particular disruptive implications for data transfers in the EU and this may affect businesses' online, digital and consumer facing operations in particular. Where to locate data centres in the future will be problematic – will Brexit lead to relocation of centres to nearby business friendly countries such as Ireland?

Whilst some international data transfers might become easier and less arduous after Brexit (e.g. to the USA) there will be a high degree of uncertainty associated with new General Data Protection Regulation which may apply during the transitionary two year negotiation period following a vote. In the meantime, companies will be in limbo which may stifle innovation and investment in the UK.

Recognised specialist expertise

Our team is regarded as one of the leading data and information practices in the UK. We recognise that integrating technological advances is essential, both to enhance the consumer experience and to help you reach consumers and maximise sales. A product of the increasingly virtual experience is that there is an increasing volume of data ('big data'), which brings with it untapped commercial opportunity and the need for more innovative ways to collect, store and exploit that data.

We advise a number of FTSE 100 and 250 companies on data privacy, related litigation, data monetisation, freedom of information, and branding issues. We are able to give cutting edge data, information and privacy advice, and have assisted clients in responding to cyber attacks (and ensuring their reputation survives too).

Our clients have expressed concern over the increase in the use of data protection rights, including subject access rights and freedom of information requests, by employees, customers, journalists and third parties such as claims management companies. To assist them, we have developed strategies to reduce the burden of requests and to deal with ICO investigations and/or the press.

Examples of our experience

- Advising a FTSE100 organisation on their implementation of Binding Corporate Rules
- Advising a global drinks company in connection with data policy and security issues arising from BYOD policies
- Advising a major building society on the creation of a single database for customers – offering a "single customer view" where all data was merged but continued to reflect varying customer preferences and consents
- Leading-edge advice in connection with some of the largest loyalty schemes a cross various sectors
- Conducting enterprise-wide data audits, including for an international recruiter (65 countries) and a sports fashion retailer
- Advising a major bank on data issues, particularly the use of geo-location data, in the context of potential mobile wallet solutions
- Rollout of Meerkat Movies (which replaced Orange Wednesdays offering weekly 2 for 1 cinema tickets) including handling privacy consents, app development and membership plans, and the collection of personal data, together with related marketing, competitions and promotions.
- Dealing with the aftermath of hacking and denial of service attacks including liaising with the police and media.
- Advising on data protection notices, telescripts, privacy policies and compliance manuals, including advising on opt-ins and opt-outs and multi-channel marketing
- Advising on investigations, enforcements, prosecutions and assessments by ICO (including a breach of PECR) and compensation claims through the courts
- Advising on the removal of information from Google using the "right to be forgotten" regime
- Advising on Data Monetisation and Data Utilisation strategies for various FTSE 100 service and retail clients with a global presence - specifically advising on risk based strategies relating to the use of big data, joint ventures, debt portfolios, customer profiling, data aggregation, legacy data and database consolidation
- Advising the NHS on the introduction of a lone worker scheme (re DPA and Human Rights Act).
- Advising the Department of Health on the renegotiation of data protection provisions in key outsourcing contracts
- Implementing a post Schrems privacy compliance regime (data transfer agreements in multiple jurisdictions).
- Advised on a 'big data' initiative to use behavioural data to enable targeted advertising in video-on-demand programmes.

Data & Information team

"Toni is a skilled negotiator & subject matter expert across all aspects of data and IT and is a strong communicator.

He remains professional and calm throughout and is a go to person for advice and opinion, not limited to legal."

ADRIAN HULL: BUSINESS PARTNER, ICT & CORPORATE PROCUREMENT AT HAMPSHIRE COUNTY COUNCIL

Toni Vitale
Legal Director
+44 (0)207 160 3158
+44 (0)7738 023372
toni.vitale@addleshawgoddard.com

Toni is a Legal Director in the Data and Information team, and joined Addleshaw Goddard from Willis Towers Watson plc, where he was Global Data Privacy Counsel. His considerable in-house experience enables him to offer practical, commercially-focused solutions in what is often a technical and complex area. After starting his career in private practice, Toni has held a number of positions as a senior legal adviser, General Counsel, Head of Legal and Company Secretary in household name businesses over the last 15 years, including IBM (where he was EMEA Data Privacy Counsel), Virgin Media, YouView TV and BGL Group (owners of comparethemarket.com).

Toni has assisted clients in the banking and insurance, retail, media and fmcg, public (including Health and MOD), and telecoms and technology sectors on a wide range of privacy and cyber security issues, including regulatory and compliance investigations, profiling, data monetisation and data breaches. He has advised on net neutrality, RIPA, location-based advertising and network integrity He has consulted with CEOP, the Home Office and NTAC on security issues and given evidence to a Joint Committee of Parliament on the Data Communications Bill. He is also an experienced technology, IT outsourcing and digital media lawyer and has led negotiations in international commercial and technology engagements.

"A star in the privacy field."

THE LAWYER

Laura Scaife
Associate
020 7160 3287
07595 085 706
laura.scaife@addleshawgoddard.com

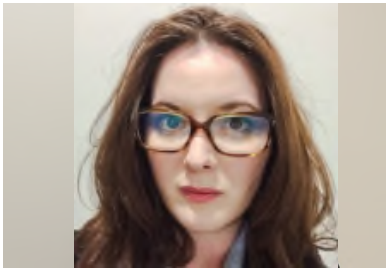
PhD candidate Laura is an expert in modern data exploitation and marketing, advising an enviable range of clients across the FTSE 100. She has been featured in **The Lawyer** as a "star in the privacy field" and "the one to watch" (Lexis Nexis and Cambridge Business School's Achievements of Women in Law 2015).

She is the author of **The Handbook of Social Media and the Law** described in peer review as the **"seminal text in the area"** and is a contributing author to Jonathan Kirk QC's **Modern Financial Regulation, Retails Digital Futures Report** and Gringras and Todd, **The laws of the Internet**.

Andrew Carter
Associate

020 71603944
07776 196703
andrew.carter@addleshawgoddard.com

Andrew qualified into Addleshaw Goddard's commercial team in September 2015 having completed his training contract at the firm. During his training contract Andrew was seconded to Barclays' Operations and Technology legal team where he advised a variety of business areas on software licensing, cloud computing, data protection and outsourcing. Andrew has acted for a range of our key clients in areas including IT, public procurement, commercial agency and consumer rights.



Rhoda Elise Bryans
Associate

020 7160 3013
07912 395544
rhoda.bryans@addleshawgoddard.com

Rhoda joined Addleshaw Goddard's Commercial team as an Associate in March 2016, after training with the firm. Her previous seats have been in Litigation (Reputation Protection), Financial Regulation (Consumer Credit) and a secondment to the Royal Bank of Scotland sitting in the Disputes and Financial Crime team. Since joining the team Rhoda has acted on a wide range of data protection matters including providing data protection assistance in Corporate acquisitions, reviewing website terms of use, privacy and cookies policies, reviewing data processing agreements and advising on data reselling arrangements. She also has experience in software licensing, non disclosure agreements, IT & Technology contracts and intellectual property.

Beatrice Duke
Associate

0113 209 2019
07730 320881
beatrice.duke@addleshawgoddard.com

Beatrice is currently on maternity leave.

Beatrice advises on a variety of Data Protection issues in wider commercial, IT and outsourcing deals, ranging from large global outsourcing agreements to website compliance and ecommerce risk. She has reviewed data protection issues in a global outsourcing deal of human resource management software for a large engineering company and drafted website Terms & Conditions and Privacy Policies for several clients (including e-commerce website and social media sites) and provided training on the Data Protection Regulation.

addleshawgoddard.com

Doha, Dubai, Hong Kong, Leeds, London, Manchester, Muscat, Singapore and Tokyo*

*a formal alliance with Hashidate Law Office