Client Alert | Intellectual Property / Technology

New restrictions on disclosures of personal data to non-EU courts will not apply in the UK

February 2016

Authors: Kathleen Hamann, Tim Hickman

One of the more controversial portions of the EU's forthcoming General Data Protection Regulation is a provision restricting the ability of EU businesses to comply with demands from non-EU courts for the production of documents containing personal data. However, following a recent announcement by the UK government, these restrictions will not apply to businesses in the UK.

The EU's forthcoming General Data Protection Regulation ("**GDPR**") contains many new provisions that are likely to prove problematic for businesses. One provision that is particularly contentious is Article 43a, which applies to any decision of a non-EU court or authority requiring an EU business to produce documents containing personal data. Article 43a states that any such decision is only enforceable if it is based on an international agreement (such as a mutual legal assistance treaty ("**MLAT**")). While MLATs are fairly common – for example, an MLAT has been in force between the US and the EU since 2010 – Article 43a would likely require courts and authorities in countries such as the US to formally submit a request pursuant to the treaty, rather than requesting the information directly from the business at issue via subpoena, search warrant, or other court order. Article 43a is sometimes called the 'anti-FISA' provision, because it appears designed to restrict the ability of non-EU courts (including the US court responsible for overseeing the Foreign Intelligence Surveillance Act of 1978 ("**FISA**"), which authorised US mass surveillance programs such as PRISM) to demand the production of documents containing personal data from businesses in the EU. However, the UK government has issued a Written Statement confirming that the restrictions set out in Article 43a will not apply to businesses in the UK.

What does this mean for businesses?

Enforcement of the GDPR is likely to begin in mid-2018. From that point onward, businesses in EU Member States other than the UK (and possibly Ireland and Denmark, as discussed further below) will be subject to the requirements of Article 43a. Those businesses may find themselves in the difficult position of having to decide whether to breach the GDPR (which includes the possibility of fines of up to €20 million or 4% of global turnover), or breach the laws of the jurisdiction whose courts are demanding the data.

US authorities, in particular, have demonstrated an increasing unwillingness to withdraw court orders and document demands because of conflicting data protection laws. In 2014, the Assistant Attorney General for the Criminal Division of the US Department of Justice ("**DOJ**"), Leslie Caldwell, noted her office's scepticism about data protection claims in other jurisdictions, inferring that they were often overblown and "obstructionist." In light of increasingly high standards for corporate cooperation under DOJ policy, as well as long-standing court opinions regarding the DOJ's ability to require production of documents even in the face of contradictory laws in other jurisdictions, refusal to produce documents because of data protection could have serious consequences in the US.

All businesses in the EU (including those in the UK) will be subject to the general restriction on cross-border data transfers imposed by Article 40 of the GDPR. In response to a demand from a non-EU court or authority that is not made under MLAT, businesses will need to implement a lawful data transfer mechanism under the GDPR (e.g., consent, Model Clauses or Binding Corporate Rules). Several of these mechanisms can be implemented significantly more quickly than the MLAT procedure, making it easier for non-EU courts and authorities to obtain timely access to documents from UK businesses than from businesses in other EU Member States. Consequently, the UK's decision not to opt-in to Article 43a may lead non-EU courts and authorities to direct their demands for data to a business' UK subsidiaries, on the basis that businesses in the UK are likely to face lower obstacles to producing the documents, together with a lower risk of sanctions for complying with such demands, and are therefore more likely to choose to produce the relevant documents.

What is the rationale behind Article 43a?

The European Commission's early unpublished drafts of the GDPR contained a provision similar to Article 43a, but that provision did not make it into the Commission's final draft, apparently as a result of intense lobbying efforts by the US government. However, following the Snowden revelations of US mass surveillance programs, that provision was reinstated in the European Parliament's draft text in March 2014. This reflects a strong political will within the EU to resist the ability of courts in the US and elsewhere to demand documents containing personal data from businesses in the EU. Unfortunately, the precise relationship between Article 43a and several other portions of the GDPR (notably Recital 90, which discusses the extraterritorial application of non-EU laws, and Article 44(1)(e), which permits cross-border data transfers for the purposes of "the establishment, exercise or defence of legal claims") remains unclear at this stage.

Why does the UK have a choice regarding Article 43a?

In general, EU Regulations (such as the GDPR) are binding on all EU Member States. However, under Protocol 21 to the Treaty on European Union and the Treaty on the Functioning of the European Union (collectively the "**Lisbon Treaty**"), the UK is not automatically subject to any EU measures that affect justice and home affairs. Whenever any provision of an EU Directive or Regulation affects justice or home affairs issues, the UK must decide whether to opt-in to that provision. If the UK decides not to opt-in, or fails to do so within three months from the date on which the provision is proposed, then the provision does not apply in the UK. The UK can subsequently make a request to opt-in to any such provision, but that request must be approved by the European Commission.

In addition, Ireland and Denmark have their own separate rights under Protocols 21 and 22 respectively, although it is not yet clear whether they intend to opt-in to Article 43a. In all other EU Member States (together with Iceland, Liechtenstein and Norway, which are subject to the GDPR by virtue of their membership of the European Economic Area) Article 43a will apply in full.

What are the consequences for the 'harmonisation' of EU data protection law?

The EU's existing data protection regime is set out in Directive 95/46/EC (the "**Directive**"). The Directive (as with all EU Directives) does not apply directly to businesses, and had to be implemented into the national laws of each Member State. Inevitably, the national legislatures of the Member States applied their own interpretations of the Directive, resulting in a 'patchwork' of similar but not identical data protection compliance requirements across the EU. Consequently, organisations trying to do business in the EU found that they were faced with data protection compliance requirements that were inconsistent (and sometimes conflicting) from one Member State to the next.

One of the core aims of the GDPR is to harmonise EU data protection law, and to a large extent it will ensure that consistent rules regarding data protection apply in all EU Member States. However, there are a number of areas in which the GDPR does not achieve full harmonisation across the EU. For example, data protection issues arising in the context of national employment law, freedom of speech and national security continue to be subject to an inconsistent 'patchwork' of national rules. Article 43a provides a further area in which there will be a lack of harmonisation, and may have a significant impact on the question of where businesses decide to store their data within the EU.

How are US authorities likely to react?

Both US courts and authorities have shown an unwillingness to move to the MLAT process to avoid data protection concerns, likely in part due to the time such requests take. The OECD, in its Typology on Mutual Legal Assistance in Foreign Bribery Cases, noted the significant hurdles posed by untimely responses to MLAT requests. AAG Caldwell, commenting in November 2015 on the recently-issued Yates memorandum regarding corporate cooperation, stated that "proactive document production, especially for evidence located in foreign countries" would be required for a business to gain cooperation credit.

US courts and authorities are likely to view the UK's decision not to opt-in to Article 43a as providing another route businesses can use to move documents to the US despite conflicting EU data protection rules – simply move the data to the UK, then move it to the US. This may well exacerbate the view of both US courts and enforcement authorities that EU data protection law does not, in fact, pose a barrier to production of documents despite the adoption of the GDPR. This view has been reinforced by the UK decision in *Madoff v. Madoff*, [2009] EWHC 442 (Ch), which US authorities have taken as blessing the movement of documents into the US for law enforcement reasons pursuant to Schedule 4 paragraph 4(1) of the UK Data Protection Act 1998.

What should businesses do now?

The conflict between EU and non-EU authorities over the application of EU data protection law in the face of lawful demands from law enforcement agencies in other jurisdictions, particularly in the US, is likely to continue to increase. Businesses, particularly those operating in digital space, should be thoughtful in designing their information architecture to account for the possibility that EU data will be demanded by non-EU courts and authorities. The UK's decision not to opt-in to Article 43a may provide an option for data storage for businesses that are likely to get caught between foreign demands and EU restrictions. However, businesses should also be mindful of the fact that Data Protection Authorities in other EU Member States are likely to take a dim view of any attempt to circumvent the application of Article 43a in those EU Member States.

It is also important to be aware that the GDPR is at least two years away from being enforced, the final text has not yet been officially published, and formal guidance on the interpretation of the GDPR has yet to be produced by EU Data Protection Authorities. Consequently, businesses should keep a close eye on developments in this area.

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000