Responding to the Challenges and Opportunities Presented by Brexit

Data Protection and Management Implications

September 2016

protiviti®
Risk & Business Consulting.
Internal Audit.

The United Kingdom (UK) voted to leave the European Union (EU) in the June 23 referendum, but the future remains uncertain with many businesses weighing the implications that will arise when the UK triggers Article 50 and formally begins the process to break away from the EU.[1] One area where Brexit could have a significant shorter-term impact is on the management and protection of personal data.

Under the existing regime, personal data can be transferred between countries within the EU, but it can only be transferred to other countries that guarantee an adequate level of protection. The new EU General Data Protection Regulation (GDPR) seeks to harmonise existing data laws and strengthen data protection rules for the digital age, where the safe storage, quick accumulation and analysis of big data is critical.[2]

Under the long-awaited GDPR, which came into force in May 2016 (although firms have until May 2018 to comply), data protection authorities can fine companies up to four per cent of global annual turnover for non-compliance. The new rules provide consumers with: greater control over how their data is used; easier access to this data; a right to data portability to protect users from having their data stored in silos that are incompatible, thereby preventing interoperability; the right to know when data has been compromised or lost; the right to be forgotten; and support for the overarching principle that systems and services should have safeguards and privacy settings built in at the design stage.

GDPR – Key Considerations

The potential impact of GDPR has focused on the challenges of implementation, the associated costs of compliance and its potential to disrupt business models. The prime concern for global organisations is, as a consequence, the likely increase in the cost of doing business in Europe at a time when many businesses are seeking to cut costs. GDPR will impact some businesses more than others and it is essential for organisations to assess quickly how GDPR will affect them. For those businesses that are more severely impacted, two years is not a lot of time to implement the required changes.

GDPR will affect every entity that holds or uses personal data about EU citizens, regardless of whether this data resides inside or outside of the EU. The extraterritorial reach of GDPR will affect organisations that do not have operations in the EU, whenever they engage with EU citizens, as, for example, customers, suppliers or employees. Therefore, organisations will need to determine the extent to which their use of personal data is impacted by the new legislation. The key consideration is not whether the company is in the EU, but whether the data that it holds, either directly or indirectly on behalf of a third party, relates to an EU citizen.

Post-Brexit Considerations

Some have incorrectly assumed that, following Brexit, GDPR will no longer apply in the UK, and have drawn the conclusion that Brexit will simplify data governance for companies in the UK. The reality is very different. Brexit actually has the potential to make the situation much more complex for organisations with operations in the UK.

In fact, the timetable for GDPR compliance is likely to run ahead of the UK's formal exit from the EU, thus there likely will be a period, albeit potentially short, when GDPR will apply in full as a result of the UK's ongoing membership of the EU. And following Brexit, the UK government will need to implement its own data protection law. Without question, there is going to be a period of uncertainty.

In any case, the EU could require the UK to demonstrate that it will continue to meet the requirements of GDPR. Discussions between the US and the EU, culminating in the Privacy Shield agreement

[1] "Brexit – What it Means and What Companies Should be Considering," Protiviti, June 29, 2016, www.protiviti.com/en-UK/Documents/Regulatory-Reports/Protiviti-Flash-report-Brexit-WhatItMeansAndWhatCompaniesShouldBeConsidering.pdf.

[2] "Reform of EU Data Protection Rules," http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

between the US and the EU, provide a possible framework.[3] As the UK currently supports GDPR and its underlying principles, it is unlikely to embrace a significantly lower standard than that adopted by the EU. So official guidance to UK companies at this stage is to "press ahead" with evaluations and plans to prepare for GDPR compliance.

It is possible, taking into account the recent comments from parliamentary committees on the matter of data protection, that the UK could adopt an even higher standard and take a very tough line by placing, for example, some level of personal accountability on senior executives.[4]

It is worth noting however that the UK's Data Protection Act 1998 (UKDPA) does not meet the requirements of the GDPR and would require significant amendment to meet the GDRP's more stringent standards.

Whatever decisions are reached, GDPR will continue to apply to any data held by organisations in the UK that relate to EU citizens. The added complication post-separation would be that a data transfer between the EU and the UK would likely constitute a "data export" under GDPR. Such data exports would come with significant restrictions, either as a result of the legislation or from restrictions in customer and/or supplier contracts.

With the significant number of unknowns relating to the direction that might be taken in the UK and the impact it might have on various organisations, there are several important things to think about now in order for organisations to position themselves to face the future with confidence.

UK government options

Post-Brexit, if the UK is not to be a part of the single market, GDPR would not have a direct effect in the UK. The UK would then have to implement its own data protection legislation and seek equivalence in order to enable the transfer of data between itself and the EU. The UK could adopt its own data protection legislation through an adjustment to the UKDPA in order to align with other EU Member States. This may be viewed as equivalent in providing the same safeguards as GDPR and enable free movement of data between the UK and EU member states. Similar status is held by countries such as Canada, New Zealand, Switzerland and Uruguay. The UK could also seek European Economic Area (EEA) membership. In this scenario, GDPR would have direct effect and the UK would be able to participate in free movement of personal data as if it were an EU Member State. It is important to stay abreast of the options available to the UK and to undertake early evaluation of the implications on organisational business models and the use of personal data. Not retaining GDPR (or at least those sections that would be applicable to a non-EU UK) could create a significant misalignment with the data protection landscape in the rest of the EU, which could prove a barrier to trade and present administrative difficulties to UK organisations.

Timing

Until the UK formally leaves the EU, organisations located in the rest of the EU will be able to continue to send and receive personal data to and from the UK. The UKDPA is based upon the European Data Protection Directive (95/46/EC). The new GDPR will be effective from May 25, 2018, and, if still a member of the EU on that date, the UK will have to comply with both the EU Directive and the GDPR. Neither the directive nor the GDPR will apply once the UK leaves the EU. Despite the Brexit vote and

---

[3] U.S. Department of Commerce, Fact Sheet: *Overview of the E.U.-U.S. Privacy Shield Framework,* www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu-us_privacy_shield_fact_sheet.pdf.

[4] The UK Parliament's Culture, Media and Sports Committee, which held an inquiry into the circumstances surrounding the breach of personal data at UK Telecom company, TalkTalk, in November 2015, recommended in a subsequent report to significantly enhance penalties for both companies and chief executives who fail to prepare for, timely report, or learn from data breaches, including tying CEO compensation to the effectiveness of their companies' cybersecurity programs.
www.publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/14805.htm.

as noted earlier, it is highly likely that organisations will have to comply with GDPR for a short period and all organisations will have to plan accordingly. The UK is likely to adopt a standard broadly equivalent with GDPR. Therefore, plans currently underway to meet the requirements of GDPR are unlikely to be a wasted effort. In fact, the Information Commissioner's Office (ICO) has stipulated that UK laws will need to be changed to make them conform to the EU's new framework to satisfy the European Commission.[5] Again, as noted earlier, UK organisations that offer goods or services into the EU or maintain data belonging to EU citizens will continue to fall within the remit of GDPR in full.

Re-evaluation of cross-border operations and data flows

Brexit could have a significant impact on data transfers between the UK and other countries. Any transfer between the UK and the EU could be deemed an export and thus subject to restrictions and/or increased regulation. Further, contractual provisions governing data transfers around the world or with third parties are likely to have been drafted on the basis that the UK was within the EU at the time of drafting. As a consequence, arrangements such as Corporate Binding Rules and/or the Privacy Shield that may have been fit for purpose prior to Brexit may no longer be appropriate. Organisations offering goods and services to EU residents or with staff or subsidiaries in the EU would, therefore, be impacted. It will be difficult to plan and to reach any meaningful conclusions before decisions are taken by the UK on its ongoing relationship with the EU and its stance on data privacy. Organisations would, however, be well advised to ensure they have a good understanding of the nature of cross-border transactions and data flows into and out of the UK. Whether this is for commercial purposes or for the management of its employees, firms will need to assess the possible implications and strategies available for managing the risks. Organisations may not have much time to react to the eventual outcome of trade and equivalence negotiations.

Repatriation of data

One possible consequence of restrictions on data transfers is that UK organisations hosting data in the EU may need to repatriate this data to the UK, while EU firms operating in the UK may need to repatriate data to EU data centers. Even if not required by GDPR, we have found significant evidence of EU companies restricting suppliers exporting personal data outside the EU, preferring not to take the risk by relying on Corporate Binding Rules or the Privacy Shield. It is also expected, in order to eliminate uncertainty, that some EU companies will demand that their suppliers move data out of the UK and into EU data centers in anticipation of their need to comply with GDPR.Taking an inventory of the location of data and developing well-thought-out contingency arrangements should data need to be repatriated are important tasks that organisations should be contemplating now.

Business change projects

All ongoing business change projects that involve a significant investment in IT should be reassessed to consider implications on data storage, transmission, etc. Given the broad definition of personal data under GDPR, almost all projects will be affected to some extent. As a priority, all organisations should evaluate their data center strategy for these projects and decide whether it might be prudent to adopt a different strategy, potentially by moving or splitting data centers across different territories in the UK and/or the EU. Organisations that make use of large cloud providers to support these projects should assess options available with service providers. While most will have arrangements for ensuring that data resides in the EU, many will not currently have arrangements in place to differentiate between the UK and the EU. Some of the larger cloud providers have already built, or are in the process of building, data centers across the EU as well as in the UK. Brexit will require many of these organisations to reevaluate their own data center strategies to ensure they are able to meet the requirements of their customers, whatever decisions are taken by regulators.

[5] "GDPR still relevant for the UK", Steve Wood, Interim Deputy Commissioner, ICO, July 7, 2016, https://iconewsblog.wordpress.com/2016/07/07/gdpr-still-relevant-for-the-uk/.

Contracts, third parties and offshore activities

Organisations should review contracts with customers and third parties in order to ascertain the "rights" agreed to retain and transfer personal data. Many contracts will have been written on the assumption that the UK is a member of the EU. For example, there could be contracts between two UK entities stating that no personal data can be exported outside of the UK. Further, contracts between data controllers and data processors should be reviewed in line with new responsibilities placed on data processes for reporting data breaches under GDPR to assess the impact on liability clauses between the contracting parties. Organisations should consider any offshore activities and evaluation of third-party suppliers as part of the scope of any review.

Training and awareness

Organisations should identify the key decision makers who are likely to require early awareness training in order to keep abreast of the potential changes in data protection legislation in the UK. This does not have to be done immediately, but it will be important to identify the key functions and individuals that will require awareness training on the potential implications of Brexit. These functions might include customer management, marketing, legal, compliance. human resources, and individual decision makers such as IT leaders, architects, programme/project managers and those responsible for negotiations with suppliers. These functions are potential high users of personal data and should be made aware of the changes under GDPR, the implications for the way they operate, and any potential new legislation that may be put in place post-separation. Ensuring that key employees are adequately aware of Brexit implications is a critical component of achieving compliance.

Our Point of View

The UK's data protection requirements are currently aligned with the principles of GDPR. Perhaps more importantly, it appears the UK legislators understand the complications that will be present for many organisations based in the UK if the government chooses not to embrace standards that are at least equivalent to GDPR. At this stage, companies should press ahead and follow formal guidance on GDPR compliance. The consensus is that the UK government will ultimately ensure the UK adopts standards that meet the requirements of the EU.

At face value, the immediate implications of Brexit on data privacy might not appear significant. However, firms should be undertaking a reassessment of their approach to managing data privacy, as a top-down, risk-based, operational change may still be required and need to be shaped. The UK already has a strong commitment to data protection, but post-Brexit, whichever regime is adopted, many UK companies are likely to experience a heightened burden of proof for compliance. In turn, the ability of the organisation to track and evidence compliance may require even more stringent controls to be adopted.

Organisations should continue to monitor the situation carefully and be ready to act if it becomes apparent that there are to be restrictions on data transfer between the UK and the EU. Although many believe this outcome to be unlikely, all affected companies need to recognise that such restrictions could be a possibility and plan accordingly. Organisations should take immediate steps to review contracts (with customers and/or suppliers). The review should ensure that where there is reference to exports outside of the EU, wording does not preclude the transfer of data.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Ranked 57 on the 2016 *Fortune* 100 Best Companies to Work For® list, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is currently working with organisations around the world to help them assess the implications of GDPR on their business and establish programs for compliance that are reflective the risk culture of the organisation and set up for success. We are currently working with organisations to perform the top-down analysis of business models to identify key risk areas and to define strategies for achieving compliance that align seek to minimise the impact on future business strategies. We recognise that there is no on size fits all approach to GDPR and that every organisation is different.

Contacts

Jonathan Wyatt
Managing Director
The Shard,
32 London Bridge Street
London
SE1 9SG
United Kingdom
+44 (0)20 7024 7522
jonathan.wyatt@protiviti.co.uk

Mark Peters
Managing Director
The Shard,
32 London Bridge Street
London
SE1 9SG
United Kingdom
+44 (0)207 3890 413
mark.peters@protiviti.co.uk

Peter Richardson
Managing Director
The Shard,
32 London Bridge Street
London
SE1 9SG
United Kingdom
+44 (0)207 024 7527
peter.richardson@protiviti.co.uk

Please note that this information is not intended to be legal analysis or advice, nor does it purport to address every issue that may impact organisations or every government response. Organisations should seek the advice of legal counsel or other appropriate advisers on specific questions as they relate to their unique circumstances.

protiviti®
Risk & Business Consulting.
Internal Audit.