Rollits LLP

Data Protection

"Brexit means Brexit"

Except when it comes to data protection

Many will have heard or seen commentary about the impending changes UK organisations will have to embrace in respect of their data protection practices pursuant to the European General Data Protection Regulation ("GDPR"). More than likely most will have put it to the back of their mind for another day. After all, the future legal landscape is somewhat opaque after Brexit, and who really knows what data protection laws will be in force once the UK eventually cuts the cord with the EU?

The GDPR is, however, fairly unique in its facts. It takes the form of a Regulation which is already in force in all EU member states without implementation of national legislation (as of 24 May 2016). Enforcement of the GDPR will not begin until 25 May 2018 and the UK's current legislation (the Data Protection Act 1998 ("the DPA")) will continue in force until that date. May 2018 may seem a long way off and some may take the view that Brexit will shield their organisation from having to invest the time and resources necessary to ensure compliance with the EU Regulation.

Bear in mind, however, that the Prime Minister only triggered Article 50 to commence the two year withdrawal process from the EU in March 2017. The GDPR will, therefore, impact organisations for at least 10 months until the UK's withdrawal from the EU has concluded. Post-Brexit, the GDPR would no longer automatically apply in the UK and the UK would have to implement appropriate data protection legislation, or (as currently seems most likely), transpose the GDPR into national legislation on the day Brexit occurs so that it effectively continues to apply.

While the above indicates that the full force of the GDPR will only potentially bite UK organisations for a relatively short period of time, the UK will no doubt wish to be in a position post-Brexit whereby it can receive personal data from controllers located in EU member states; for example, UK organisations with EU customers. This means the UK will need to ensure that its data protection laws provide an adequate level of protection for personal data by EU standards. The European Commission can examine the laws of a country located outside the EU to determine whether that country's data protection laws are adequate and (if they are) formally recognise them as such by issuing an "Adequacy Decision". Personal data can be transferred to countries outside the EU who have received an Adequacy Decision (known as White List countries) on the same terms as if the recipient were located in the EU.

The UK might seek to obtain an Adequacy Decision during the withdrawal negotiations, but such a decision is only likely to be forthcoming if the data protection laws adopted by the UK offer equivalent protection to the GDPR. This would require the DPA to be amended or replaced.

Regardless of the above, due to the territorial reach of the GDPR, UK organisations which offer goods or services to, or monitor the behaviour of, data subjects in the EU (which will include most businesses with an online presence) will still have to comply with the GDPR irrespective of what UK laws are in place.

Elizabeth Denham, the new UK Information Commissioner, has commented that organisations should continue to make arrangements to comply with the GDPR and made the following comments to the BBC in September 2016:

"I don't think Brexit should mean Brexit when it comes to standards of data protection… In order for British businesses to share information and provide services for EU consumers, the law has to be equivalent."

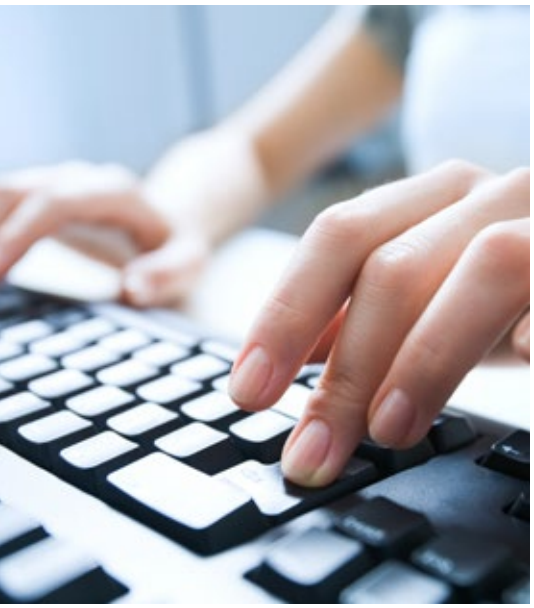
Continues overleaf...

HULL 2017 UK City of Culture
CITY PARTNER

"Brexit means Brexit"… except when it comes to data protection

A speech by Secretary of State Karen Bradley MP in October 2016 has further confirmed the UK Government's current position:

"We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public."



It therefore appears that Brexit does not mean Brexit when it comes to data protection and it is looking increasingly likely that the high standards imposed by the GDPR will be adopted into UK law. Organisations which are currently complying with the DPA will be in a strong starting position to address the changes required by the GDPR. Nevertheless, identifying and implementing any changes necessary pursuant to the GDPR is likely to require a substantial lead time. UK organisations therefore need be proactive in reviewing and (if necessary) updating their data protection policies and procedures in light of the GDPR and should ensure that appropriate training is provided to staff before the GDPR becomes enforceable.

The need for reform

1995 may be remembered for a number of reasons: the PlayStation was introduced to the world; Blackburn Rovers stormed to victory in the Premier League; Robson and Jerome spent seven weeks at number one for their rendition of Unchained Melody; and (for a few people at least) data protection suddenly became interesting as a result of the introduction of the EU Data Protection Directive ("the Directive").

The DPA implemented the Directive in the UK five years later and it is a piece of legislation which most organisations will, to some degree, be familiar with. Since the Directive was drafted, technology and the way that we communicate and interact has developed substantially. Social web and mobile technologies have accelerated the rate at which information is shared to a level which can be challenging to keep up with. The number of people with access to the internet has increased exponentially and we are now able to maintain instantaneous communication with global contacts via applications such as Facebook, WhatsApp, Twitter, Snapchat and LinkedIn.

Advances in information technology have not, however, been matched by advances in data protection law resulting in outdated legislation which is not sufficiently sophisticated to deal with today's technological landscape.

Personal data is a valuable commodity and the increase in sharing and use of personal data in order to access the plethora of goods and services available has also led to an increase in large-scale misuse of such personal data. The ICO has sought to clamp down on misuse of personal data by issuing large fines against organisations that have breached their data protection obligations. Media coverage exposing data protection breaches has also become commonplace, thereby increasing the reputational damage which accompanies a data protection breach. Recent examples include the following:

- TalkTalk was fined £400,000 for failing to prevent a cyber attack which resulted in the attacker gaining access to the personal data of 156,959 customers.
- Chelsea and Westminster Hospital NHS Foundation Trust was fined £180,000 for revealing the email addresses of more than 700 users of an HIV service when sending a newsletter by email to the recipients using the 'to' field instead of the 'bcc' field.
- Blackpool Teaching Hospitals NHS Foundation Trust was fined £185,000 for inadvertently publishing the private details of 6,574 members of staff on the Trust's website.
- A medical practice in Hertfordshire was fined £40,000 after releasing confidential information about a patient and her family without permission. The patient had warned that staff should take particular care to protect her details; however the information was nevertheless released in response to a subject access request made by the patient's estranged ex-partner. The subsequent ICO investigation found that the practice had insufficient systems in place to safeguard patients' personal data and that staff were not properly supervised or trained in respect of data protection.

Despite the threat of a substantial fine being issued by the ICO for a data protection breach, not all organisations adequately address their data protection obligations and allocate sufficient time and resources to ensure that personal data is adequately protected. This may, in part, be due to some organisations considering the risk of enforcement action for a data protection breach to be relatively low in the pecking order of other risks that their organisation is potentially exposed to. Some have learned at great financial and reputational costs that the risk assessment was wrong.

Due to the above, and the divergent approaches taken by the different EU member states in implementing the Directive, it was decided that reform was needed. Four years of debate, negotiation and lobbying then ensued culminating in the GDPR, which seeks to modernise and homogenise the law and strengthen the protection granted to EU citizens in respect of their personal data.

Information

If you have any queries on any issues raised in this document please contact David White on 01482 337209.

This is for the use of clients and will be supplied to others on request. It is for general guidance only. It provides useful information in a concise form. Action should not be taken without obtaining specific advice. We hope you have found this useful. If, however, you do not wish to receive further mailings from us, please write to Pat Coyle, Rollits, Citadel House, 58 High Street, Hull HU1 1QE.

Hull Office
Citadel House, 58 High Street,
Hull HU1 1QE
Tel +44 (0)1482 323239

York Office
Forsyth House, Alpha Court,
Monks Cross, York YO32 9WN
Tel +44 (0)1904 625790

rollits.com

Authorised and Regulated by the Solicitors Regulation Authority under number 524629

Rollits is a trading name of Rollits LLP. Rollits LLP is a limited liability partnership, registered in England and Wales, registered number OC 348965, registered office Citadel House, 58 High Street, Hull HU1 1QE

A list of members' names is available for inspection at our offices. We use the term 'partner' to denote members of Rollits LLP.

May 2017