RegulatoryStrategies working with CICM Chartered Institute of Credit Management

UK Data Protection Newsletter July 2016

Headlines this month:

- Brexit and the General Data Protection Regulation (GDPR)
- Illegal trading of personal data
- Recent data breaches
- EU update

Commentary:

Brexit and the General Data Protection Regulation (GDPR)

The decision to leave Europe has raised questions about what the future holds for the UK in relation to data protection. The ICO has stated that we will clearly need to adopt a model that mirrors the GDPR whatever the final outcome of the Brexit negotiations. Certainly, we know that the GDPR will come into force on the 25th May 2018 and the UK will probably need to comply with it for a period of time which will be determined by when we invoke Article 50. Commentators on the GDPR are consistently urging organisations to continue with plans to comply with the regulation.

The ICO has issued the following statement in response to the outcome on the 23rd June:

"The Data Protection Act remains the law of the land irrespective of the referendum result.

"If the UK is not part of the EU, then upcoming EU reforms to data protection law would not directly apply to the UK. But if the UK wants to trade with the Single Market on equal terms we would have to prove 'adequacy' - in other words UK data protection standards would have to be equivalent to the EU's General Data Protection Regulation framework starting in 2018.

"With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organisations and to consumers and citizens. The ICO's role has always involved working closely with regulators in other countries, and that would continue to be the case.

"Having clear laws with safeguards in place is more important than ever given the growing digital economy, and we will be speaking to government to present our view that reform of the UK law remains necessary."

Regulatory Strategies sent the following out to clients in light of the decision and we will

continue to monitor the situation:

"With today's 'Brexit' decision, the following is a very early view of the potential impacts on legislative and business impacts.

"In summary, ultimately the UK's post-Brexit business and legal landscape will largely depend on the nature of our continued relationship with the EU, and the scope and type of changes we decide to make to our legislation.

"Using the data protection GDPR as an example. However the EU legislative framework applies equally to all many area of UK financial services law.

"The data protection framework in the EU and UK is based on the Data Protection Directive. This is a common approach across many areas of UK business and employment law where EU Directives are transposed into member state legislation and in the case of EU Regulations, these apply directly to members states without the need to enact them into an Act of Parliament – to use the UK as an example.

"Although member state regulation is based on this Data Protection Directive, domestic laws and, in particular, respective enforcement practices differ to some extent from one state to another.

"A higher degree of harmonisation in EU data protection standards will be achieved by the upcoming General Data Protection Regulation (GDPR), which will most likely come into force in 2018. The GDPR will be directly applicable in all member states, and will introduce fines at a level similar to antitrust regulations in the EU. It will have a broad scope of application as it will also cover data processing outside the EU if such processing is related to the offering of goods or services to data subjects in the EU.

"The transfer of personal data outside the EU is subject to additional requirements. In most cases, this is only allowed if the country where the recipient of the data is located is regarded as a 'safe third country' by the European Commission. This is where the UK is very likely to follow similar lines to those contained in the GDPR irrespective of no longer being in the EU post the Article 50 process.

"An important question is whether, after Brexit, the UK would be classified as a 'safe third country' by the Commission, so as to permit EU personal data to be transmitted to the UK. If it were not, UK companies doing business in the EU would need to re-think their data protection compliance strategy.

"Cross-border data flows to data processors in the UK that do not currently require a legal justification are likely to require a particular justification in case of a Brexit. Without such justification, changes to data flows will become necessary. This would be especially burdensome if the data processor plays a role as a data processing hub within a group structure with headquarters or subsidiaries in the EU.

"This need to follow EU legislative expectations cuts across many areas of UK business and even being outside the UK will require the UK to adopt acceptable levels of controls and safeguards to ensure our ongoing ability to trade with the EU and its member states. In short, economic and commercial drivers will dictate how much we follow EU legislation, rather than political considerations and the desire to be independent.

"There are a number of possible models already in operation for non EU countries.

"When the UK leaves the EU it could join the European Free Trade Association and remains part of the European Economic Area (EEA)? (the Norwegian option)

"The four freedoms as laid down in the Treaty on the Functioning of the European Union (ie the free movement of goods, services, persons and capital, as well as competition and state aid rules) are incorporated in the EEA Agreement. This means that:

- *the Data Protection Directive applies throughout the EEA. Hence, nothing would change since the UK would still have to comply with this directive; and*
- *the upcoming GDPR would have an immediate effect on UK-based companies.*

"When the UK leaves the EU w it does not adopt any form of free trade agreement? (the WTO option)

- *The UK would be free to revise its data protection framework and deviate from EU standards.*
- *The upcoming GDPR would have no direct effect on the UK.*
- *Depending on future revisions to UK data protection law, the Commission would have to designate the UK as a 'safe third country'. If it didn't, data transfers to the UK would be subject to stricter requirements, like data transfers to the USA, for example.*

"The above would apply equally to all current and pending EU Directives and Regulations applicable to EU member states.

For further information contact Mike Bradford or Helen Lord at Regulatory Strategies
consultancy@regulatorystrategies.co.uk

"It will be a turbulent time on all fronts and things will only becomes clearer once the EU exit discussions start, probably after October when a new PM will be elected."

Baroness Neville-Rolfe, whose brief includes data protection policy, has commented at the recent Privacy, Laws and Business conference that the future is uncertain but the reality on which policy is based has not changed much.

The ICO has taken the view that it is still relevant to publish its overview of the GDPR because, regardless of exactly what happens, it will still be relevant to many UK companies. The ICO commented this week that:

"With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organisations, and to consumers and citizens. The ICO's role has always involved working closely with regulators in other countries, and that will continue to be the case. Having clear laws with safeguards in place is more important than ever given the growing digital economy, and we will be speaking to government to explain our view that reform of UK data protection law remains necessary."

The Direct Marketing Association (DMA) has provided the following advice to its members:

"Leaving the EU does not mean UK marketers should abandon the route to compliance with the GDPR. The UK will want to continue trading with the EU, so our data protection law will need to be broadly equivalent to existing legislation."

Illegal trading of personal data

The ICO has made raids on houses in Sheffield and Manchester as part of investigations into the illegal trading of personal data.

The webinar touches on disproportionate effort, what controllers can require before responding to a request and how to deal with requests when third party The investigation in Sheffield has suggested that people living at the addresses could be selling marketing lists to companies involved in nuisance calls.

The Manchester raid was prompted by information suggesting that the person living at the address was unlawfully accessing personal information which is a Section 55 offence.

is involved.

Recent data breaches

Change and Save Limited

The ICO has issued a 'stop order' against a company that was falsely claiming it was phoning people as part of a lifestyle order. This practice is known as "sugging". The company claimed that it could call people registered on the Telephone Preference Service (TPS) because its survey was not subject to direct marketing rules. However, the ICO received a number of complaints that the calls went on to promote other services.

Advanced VoIP Solutions Limited

The ICO has imposed a £180,000 monetary penalty further to an investigation prompted by over 6,000 complaints relating to recorded messages. The messages were in relation to personal protection insurance, packaged bank account and flight delays.

The ICO has commented:

"The number of complaints in this case is just a drop in the ocean compared to the millions of calls we thing this company has made.

"We have sent out a clear message to companies who behave in this way – however much you try and dodge the law, it won't work, and we will act".

Quigley and Carter Limited

2,600 complaints over two months, has resulted in a £80,000 fine for a company breaking direct marketing rules. The company had sent marketing texts to individuals who had not consented to receive them and it did not have a direct relationship with them.

Central Compensation Office Limited

The Central Compensation Office Limited has been ordered to stop making nuisance calls or face legal action. Calls were made to people registered with the TPS and who had not consented to receive them.

The ICO has issued an enforcement notice, failure to comply with which is a criminal offence.

Dyfed-Powys Police

A police force has been fined £150,000 after it was found to have failed to have processes in place to keep personal information secure. The lack of appropriate measures was identified after an email was erroneously sent to a member of the public containing information that could have been used to identify eight sex offenders.

EU update

RegulatoryStrategies

The below provides an EU update from Brussels, and provides an insight into the progress of the EU's draft data protection regulation:

This month saw the EU-US Privacy Shield agreement negotiations back on track towards a swift final approval after the setbacks in the discussions experienced in May. The EU-US Privacy Shield is designed to replace the Safe Harbour agreement which had been struck down by the European Court of Justice last October. A first political agreement reached in February had been criticised over the past months by Members of the European Parliament, the European Data Protection Supervisor, national data protection authorities and NGOs which all expressed their doubts over the text's loopholes.

In order to tackle their critics, the European Commission entered into new negotiations with US officials and struck a new deal on 25 June. The final changes in the text seek to address the concerns raised by the Article 29 Working Party – which is composed of European national protection authorities – in their 14 April non-binding opinion. According to the revised agreement the US put in writing their commitment that bulk collection of data would only occur under specific circumstances and that it would be 'as targeted and focused' as possible. US counterparts also clarified the role of the new US Ombudsman and the fact that he/she would be independent from US national security services. Another amendment aimed at requiring companies to delete data which no longer serves the purpose for which it was collected.

The European Commission is confident that EU Member States will back the new text by the beginning of July. Its plan is to adopt the new agreement at the weekly College meeting on 5 July in order to have the EU-US Privacy Shield up and running before the summer recess.

However, the business community does not seem to have bought the deal as they fear that a weak – how they define it – Privacy Shield agreement would create more uncertainty and increase the possibility of having data transfers ruled illegal by European judges.

While the EU-US Privacy Shield would now cover only 27 EU Member States, with the UK having decided to leave the EU in the light of the results of the UK's EU referendum held on 24 June, London would be required to adopt similar terms in the near future if it wants to trade with the EU. As set out in a statement issued by the UK Information

For further information contact Mike Bradford or Helen Lord at Regulatory Strategies
consultancy@regulatorystrategies.co.uk

Commissioner's office: "If the UK wants to trade with the single market on equal terms we would have to prove 'adequacy' – in other words, UK data protection standards would have to be equivalent to the EU's General Data Protection Regulation framework starting in 2018".

June also saw the signature of the EU-US Umbrella Agreement which was agreed on by the two shores of the Atlantic in September 2015 and which includes data protection measures for data transfers for law enforcement purposes, including terrorism. The agreement was signed on 2 June by Dutch minister Ard van der Steur and Commissioner Jourová on behalf of the EU and by Attorney General Loretta Lynch on behalf of the US authorities.

Visit our website at www.regulatorystrategies.co.uk

For further information contact Mike Bradford or Helen Lord at Regulatory Strategies
consultancy@regulatorystrategies.co.uk