ALERT MEMORANDUM

Some reflections on: Brexit and the U.K. Data Protection Regime

August 15, 2016

Prior to notice being given under Article 50 of the Treaty on the European Union (the "exit" mechanism for departure of a Member State), and for up to two years thereafter, the result of the UK's referendum of June 24, 2016 to leave the EU ("**Brexit**") will have no direct impact on data protection law in the UK. More importantly, it is likely that businesses in the UK will face a data protection and cyber security landscape heavily influenced by EU law for the foreseeable future. The EU General Data Protection Regulation[1] ("**GDPR**") entered into force on 24 May 2016 and takes full effect at the end of a two-year transitional period expiring on 25 May 2018. The GDPR will therefore, most likely become applicable to the UK prior to the UK ceasing to be a member of the EU.

The regulation of data protection in the UK post-Brexit is, however, uncertain in the longer-term. The future UK data protection regime will be guided by the relationship the UK Government negotiates with the EU and whether, for example, the UK's continued access to the single market requires the UK to retain the GDPR or to enact equivalent legislation. As a matter of policy, UK law would be likely to impose a broadly equivalent level of data protection to that applied in the GDPR, even if only to ensure that the UK is deemed an "adequate jurisdiction" in EU terms, thus securing the viability of data flows from the EU. However, even if laws equivalent to the GDPR are enacted in the UK, companies that process personal data in the UK will not be able to benefit from the "*One Stop Shop*" mechanism under the GDPR; accordingly, such companies would be forced to deal with more than one data protection regulator and the divergent enforcement styles of each. Should the UK introduce its own data protection regime, the extra-territorial reach of the GDPR will mean that UK businesses will be required to comply with the EU regime in any event, in respect of any processing of personal data belonging to EU residents.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors:

LONDON
City Place House
55 Basinghall Street
London EC2V 5EH, England
T: +44 20 7614 2200

Simon Jay
+4420 7614 2316
sjay@cgsh.com

Colin Pearson
+44 20 7614 2390
cpearson@cgsh.com

Gareth Kristensen
+44 20 7614 2381
gkristensen@cgsh.com

PARIS
12, rue de Tilsitt
75008 Paris, France
T: +33 1 40 74 68 00

Fabrice Baumgartner
+33 1 40 74 68 53
fbaumgartner@cgsh.com

Emmanuel Ronco
+33 1 40 74 69 06
eronco@cgsh.com

BRUSSELS
Rue de la Loi 57
1040 Brussels, Belgium
T: +32 2 287 2000

Christopher Cook
+32 22872137
ccook@cgsh.com

Natascha Gerlach
+32 2 287 2201
ngerlach@cgsh.com

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (*General Data Protection Regulation*). For additional information on the GDPR, please refer to our May 13, 2016 alert memorandum: https://www.clearygottlieb.com/~/media/cgsh/files/alert-memos/alert-memo-pdf-version-201650.pdf

I. UK after leaving the EU

Consequences of the UK referendum.

The referendum result will not give rise to the UK's immediate exit from the EU; the "leave" vote must be given effect by the UK government, who can trigger the Article 50 mechanism by delivering a notice of the UK's intention to leave the EU to the European Council. The service of the notice triggers a two year negotiation period during which the UK and the EU would have the opportunity to conclude an agreement for the withdrawal of the UK and agree a post-Brexit framework, among other things, for trade between the UK and the EU.[2] The UK would remain a member of the EU and continue to be subject to EU law until the expiry of this negotiation period.

Importantly, irrespective of when the Article 50 mechanism is triggered, the two year negotiation period will most likely not end prior to the full implementation of the GDPR on May 25, 2018. Therefore, the UK will be required to comply with the new regulation for at least a short period, whatever the outcome of the upcoming UK-EU negotiations.

Going forward, the UK's data protection environment will be shaped by the relationship which the UK negotiates with the EU. Participation in the single market will, for example, require implementation of the GDPR on a long-term basis. The various models and their implications for the future of UK data protection are further discussed below.

EEA Model.

Members of the European Economic Area (the "**EEA**") benefit from trade arrangements which allow them to be part of the single market, without full membership of the EU. There are currently three EEA members, Norway, Liechtenstein and Iceland; these countries enjoy the benefits of free movement of goods, services, people and capital and are accordingly required to comply with fundamental EU rules (i.e., EU legislation concerning employment, competition policy and consumer protection including data protection rules). The EEA members have therefore implemented the Data Protection Directive[3] and the e-Privacy Directive[4] into local law.

As an EEA member, the UK would be legally obliged to retain the Data Protection Act 1998 ("**DPA**") (which implements the Data Protection Directive into UK law). The UK would also need to give effect to the GDPR in due course, in order to be permitted access to the single market.

Swiss Model.

Neither a member of the EU nor the EEA, Switzerland has instead negotiated bilateral agreements with the EU which govern the Swiss-EU relationship. Switzerland is a member of the European Free Trade Association ("**EFTA**"), which provides for free trade between the EU and Switzerland for all non-agricultural goods.

The Swiss model allows Switzerland to choose which EU initiatives it participates in. However, Switzerland is required to implement laws, which track EU legislation, in order to continue benefitting from free trade with the EU. The UK could adopt a similar approach, in which case the effect on data protection regulation would depend on the degree of access to the single market that the UK chooses to negotiate with the EU. If the UK wishes to establish a level of free trade similar to Switzerland, compliance with EU data protection laws (including the GDPR) would be inevitable.

Free Trade Agreements.

Similar to the approach adopted by Canada, the UK could seek to negotiate with the EU on an independent basis (outside of the EEA, EFTA and WTO models (see below)). This would give the UK freedom to

[2] Strictly, the negotiations between the UK and the EU could result in the UK's exit in less than two years; alternatively, the period could be greater than two years with the unanimous consent of the remaining twenty seven Member States.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

establish the extent of its relationship with the EU including with respect to data protection. Under this model, the UK could reform data protection laws to its own specification.

However, as discussed further below, divergence from EU principles of data protection are likely to have implications for EU-UK data flows and transfers of EU data subjects' personal information from the UK to other "third" countries. Questions as to the "adequacy" of the UK data protection regime will arise, which could have a significant impact on some sectors of the UK economy (particularly financial services).

WTO Model.

The UK may rely on its membership of the World Trade Organization ("**WTO**") in order to trade with the EU. Under such a model, the UK would not have access to the single market; accordingly, the UK would be under no obligation to adopt EU regulation or implement EU directives into national law.

Like the Free Trade Agreements option, the WTO model would give the UK freedom to design its own data protection reforms, but would similarly give rise to issues surrounding adequacy and data transfers should the UK diverge from the GDPR in any significant way (see below for further information).

UK's ability to influence EU data protection law

- The UK Information Commissioner's Office (the "**ICO**") currently represents the UK's interests within the Article 29 Working Party (i.e., the group of representatives from national data protection authorities across the EU, the European Data Protection Supervisor (the "**EDPS**") and the Commission, who issue opinions on key data protection issues, the "**Working Party**").
- The Working Party's influence and guidance is likely to become of increasing importance as we approach May 25, 2018, at which point the GDPR will enter full force.
- The GDPR will establish the European Data Protection Board (the "**EDPB**"), which will supersede the Working Party, comprising a representative from each Member State and the EDPS. The EDPB will provide EU wide guidance on the application and interpretation of the GDPR and will also be responsible for the resolution of disputes and the implementation of certification schemes.[5]
- Following the expiration of the two year period under the Article 50 mechanism, the ICO will no longer be eligible for membership of the EDPB. In the interim, while the finer details of the GDPR are still being developed by the Working Party, the ICO will inevitably have less influence over Working Party discussions.
- If the UK, by whatever model, chooses to implement or track EU data protection standards, it will not be able to shape legislative changes as it did as a member of the EU.

II. Position of the UK Information Commissioner

Statement of the ICO: April 19, 2016.

Prior to the referendum, the ICO set out the UK's need for robust data protection laws, irrespective of its EU membership. The ICO highlighted the UK's historic commitment to data protection, noting that UK data protection laws "*precede EU legislation by more than a decade, and go beyond the requirements set out by the EU*".[6]

[5] Please see Chapter 6, Section 3 of the GDPR.

[6] ICO statement of April 19, 2016 "*Statement on the implications of Brexit for data protection*" (https://ico.org.uk/about-the-ico/news-and-

Statement of the ICO: July 1, 2016.

In a post-referendum statement, Christopher Graham, former UK Information Commissioner, explained that:

- "*With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organizations 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 present our view that reform of the UK law remains necessary*."[7]

Is the GDPR still relevant?

- Despite the referendum result, the ICO has restated its commitment to producing a set of guidance on the GDPR, confirming its continuing relevance to the UK.
- In particular, the ICO has noted the importance of GDPR compliance for UK organizations operating on an international basis.
- While acknowledging that the future of UK data protection law, post-Brexit, is uncertain, Interim Deputy Commission Steve Wood has stated that the "*underlying reality on which policy is based has not changed all that much*".[8]

III. Reform of the UK Regime

It is not yet clear what approach the UK will take to data protection, post-Brexit. If the UK intends to remain a beneficiary of the single market, it will likely be required to comply with EU data protection law or demonstrate that it adequately protects personal information (i.e., to at least the standards prescribed under EU law).

The "adequacy" of UK data protection law.

The importance of adequacy is far reaching. Not only would the UK's ability to participate in the free market be impacted by a divergence from EU standards, but it would also impact EU to UK data flows.

- Personal data may be freely transferred between EEA Member States. Should the UK decide to negotiate a trade deal with the EU outside of the EEA framework, it would be considered a "third" country under EU data protection law.
- Transfers of personal data to third countries are permitted in limited circumstances only. For example, where (i) transfers are subject to appropriate safeguards (such as the EU standard contractual clauses (the "**Model Clauses**") or binding corporate rules between various entities in a multinational organization (the "**BCRs**")), or (ii) on the basis of a Commission finding of adequacy.[9]

The Commission has found a number of countries to be adequate, including Switzerland and Canada. Should the UK decide to take a lighter touch to data protection, it is unlikely that the Commission would see fit to grant the UK a similar finding of adequacy.

Furthermore, following the October 2015 decision of the Court of Justice of the European Union (the "**CJEU**") in *Maximillian Schrems v Data*

events/news-and-blogs/2016/04/statement-on-the-implications-of-brexit-for-data-protection/)

[7] ICO statement of July 1, 2016: "*Referendum result response*" (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/07/referendum-result-response/)

[8] ICO blog, July 7, 2016: "*GDPR still relevant for the UK*" (https://iconewsblog.wordpress.com/2016/07/07/gdpr-still-relevant-for-the-uk/)

[9] For the full list of countries deemed adequate by the Commission, please visit http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Protection Commissioner ("***Schrems***"),[10] the Commission is unlikely to consider a country adequate where its domestic law permits the mass surveillance and retention of data. In light of the *Schrems* jurisprudence, the existence of legislation such as the Data Retention and Investigatory Powers Act ("**DRIPA**"), under which the UK Government can force communications companies to retain data for twelve months for access by public authorities, may jeopardize an adequacy finding in favor of the UK.[11] Additionally, the introduction of new legislation which allows for mass data retention and surveillance of data without strict limitations, for example the Investigatory Powers Bill (also known as the "*Snooper's Charter*"),[12] may also weaken the chances of an adequacy finding being made.

IV. Implications for UK Businesses

Loss of the "one stop shop" mechanism.

The GDPR introduces a "*One-Stop Shop*" mechanism designed to allow organizations established in multiple Member States to deal with one supervisory authority only. While all supervisory authorities will be competent to hear complaints affecting data subjects or establishments in that relevant Member State the organization itself can liaise with the supervisory authority in its main establishment only, streamlining the regulatory process.

Outside of the EU, the UK will not be able to take advantage of this mechanism. This would add to the administrative burden of UK based businesses who would be required to liaise with supervisory authorities in each of the Member States in which they do business and potentially face parallel investigations from EU and the UK authorities. If the UK varies the approach it takes to data protection from that taken within the EU, these organizations will also have to ensure compliance with two different regimes.

Territorial scope of the GDPR – appointment of representatives.

Where an organization established outside of the EU processes the personal data of EU citizens in the course of its business ("**Non-EU Controllers**"), it will be caught by the extra-territorial reach of the GDPR.[13] Therefore, businesses established in the UK may have to comply with the GDPR despite the UK's exit from the EU and irrespective of the relationship the UK negotiates with the EU going forward.

Additionally, the GDPR requires Non-EU Controllers to designate a representative in the EU.[14] The representative must be established in one of the EU Member States where relevant data subjects are located and will act as a point of contact on behalf of the Non-EU Controller, in respect of all issues relating to compliance with the GDPR.

Transfers of data from the EU to the UK.

As detailed above, after its exit from the EU, the UK will be considered a third country for data protection purposes. Businesses wishing to transfer personal data to the UK will therefore have to first ensure such a transfer is compliant with EU law.

If the UK aligns its data protection regime with the GDPR, it is possible that the Commission will make an adequacy decision in the UK's favor, allowing for the transfer of data from the EU to the UK without the need for additional safeguards.

[10] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015.

[11] Data Retention and Investigatory Powers Act 2014. The CJEU are currently scrutinizing the legality of DRIPA; a judgment is expected later this year.

[12] The Investigatory Powers Bill is currently at the House of Lords' committee stage; the progress of this Bill can be tracked here: http://services.parliament.uk/bills/2015-16/investigatorypowers.html

[13] Article 3 of the GDPR extends the scope of the regulation to controllers (i.e., the body that, alone or jointly with others, determines the purposes and means of processing of personal data) and processors (i.e., a body which processes personal data on behalf of a controller) whose processing activities relate to the offering of goods and services or the monitoring of behaviours, of data subjects in the EU.

[14] A representative is not required if data processing: (i) is occasional, (ii) does not extend to the processing of special categories of data (such as biometric data, criminal convictions and/or details of an individual's race, ethnicity, political or religious opinions or sexual orientation) on a large scale, and (iii) is unlikely to result in a risk to the rights and freedoms of natural persons taking into account the nature, context, scope and purpose of the processing.

Should such a decision not be given, transfers to the UK could be effected under a bespoke EU-UK "*safe harbor*" or "*privacy shield*" (as is the approach taken to EU-U.S. transfers of personal data).[15] Such a mechanism would require UK businesses to sign-up, and adhere, to the additional rules set out under such a framework. Alternatively, organizations could rely on Model Clauses or BCRs. Model Clauses are however not ideally suited to regular data flows and were intended for ad hoc data transfers; the BCRs are administratively burdensome to put in place and not available to organizations who do not operate on a multi-national basis.

Transfers of data from the UK to the U.S.

Transfers of personal data from the EU to the U.S. were previously permitted where a U.S. based organization was certified under the EU-U.S. Safe Harbor.[16] The CJEU invalidated the Safe Harbor adequacy decision following the the *Schrems* complaint, which questioned the adequacy of the protection afforded to EU data subjects' personal information when transferred to the U.S.[17] The EU and the U.S. have subsequently agreed a new framework, the EU-U.S. Privacy Shield.[18]

A post-Brexit UK would need to consider putting in place a UK-U.S. "privacy shield" in order to be considered as providing adequate protection for EU data subjects' personal information. Without such a mechanism in place, data intended to be transferred to the U.S. could be transferred via the UK (where the UK has been deemed adequate by the Commission) and subsequently onto the U.S., thus circumventing the EU's prohibition on such transfers.

By way of example, Switzerland (which has been deemed a country of adequate protection by the Commission) previously effected transfers of personal data to the U.S. under the Swiss Safe Harbor framework.[19]

V. Advice for UK Businesses

The UK will continue to be a member of the EU in the short term and the referendum will not have an immediate impact on data protection in the UK. The DPA will remain the main piece of UK legislation applicable to organizations which process personal data in the UK until the GDPR comes into full force in May 2018. Data transfers between the UK and EU may continue without the need for additional safeguards until such a time that the UK is considered a third country for EU data protection purposes.

Businesses in the UK should continue to apply the DPA, while simultaneously preparing themselves for the new GDPR regime over the next year and a half.[20] The importance of full compliance with the GDPR should not be understated due to Brexit, given the likelihood of a UK regime which mirrors the GDPR's requirements and the extra-territorial reach of the GDPR in any event, for businesses who process the personal data of EU residents.

Despite the fact that alignment with the EU data protection regime is likely to be necessary in order to be deemed a country of adequate protection (so as not to jeopardize data transfers from the EU to the UK), UK businesses should be sensitive to any divergence between the UK and EU regimes going forward, in

[15] For additional information on the EU-U.S. Privacy Shield, please refer to our August 2, 2016 alert memorandum: https://www.clearygottlieb.com/~/media/cgsh/files/alert-memos/alert-memo-pdf-version-201679.pdf

[16] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (the "**Safe Harbor adequacy decision**").

[17] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015.

[18] Commission Implementing Decision of 12.07.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

[19] Following the CJEU's decision in *Schrems*, the Federal Data Protection and Information Commissioner of Switzerland (the "**FDPIC**") declared that the Swiss Safe Harbor no longer provided sufficient protection for data transferred from Switzerland. Furthermore, in order to ensure that data flows from the EU to Switzerland were not jeopardized, the FDPIC removed the US from its list of countries with adequate protection. Additional information can be accessed at: https://build.export.gov/main/safeharbor/swiss/eg_main_018519

[20] For additional information on the GDPR, please refer to our May 13, 2016 alert memorandum: https://www.clearygottlieb.com/~/media/cgsh/files/alert-memos/alert-memo-pdf-version-201650.pdf

order to avoid being caught out. Resources will need to be invested in monitoring updates and legislative changes and ensuring compliance with both regimes where personal data is collected in relation to both UK and EU data subjects.

To the extent that the Commission decides that the UK regime does not provide adequate protection for personal data, or there is a delay after Brexit in the Commission taking such a decision, UK businesses will need to be ready to put other safeguards in place, so that there is no disruption to their cross-border data flows. UK based organizations should consider assessing whether Model Clauses or BCRs would be appropriate in the time leading up to the UK's exit from the EU.

…

CLEARY GOTTLIEB