SLAUGHTER AND MAY

Data Protection and Privacy Newsletter

January 2019 / Issue 10

Selected legal and regulatory developments in data protection and privacy

Quick Links

Since our last edition, the data privacy focus has continued to shift from GDPR preparation to the operational challenges of ongoing compliance, with all eyes watching the Brexit-brinkmanship.

At the beginning of December we held our annual Data Protection and Privacy Forum and were delighted to see so many of you there. We were joined by Richard Sargeant, one of the newly appointed board of the Centre for Data Ethics and Innovation, for an optimistic opening address on the potential of AI. Attendees at the Forum went on to discuss their practical approaches to direct marketing, data breach reporting, automated processing and the privacy issues raised by commercial transactions. If you would like any further details on our Forum discussions, please let us know.

This year, unsurprisingly, we asked Forum attendees about their Brexit preparations. Interestingly, 51% of attendees planned to put model clauses in place as a contingency measure for a no-deal scenario, and 14% intended to move servers to Europe. However, only 36% of attendees had started implementing their contingency plans ahead of the publication of the (now rejected) Withdrawal Agreement. Attendees discussed that although Brexit poses challenges for data flows, the work done on GDPR compliance projects will stand them in good stead to adapt to regulatory changes.

With the ICO set to lose its seat on the European Data Protection Board (EDPB) in (almost) any Brexit scenario, it is, however, encouraging to see that the ICO has taken steps to remain at the forefront of the global data protection scene. In October, when Elizabeth Denham was announced as the new chair of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) she said: "*The ICDPPC is a truly unique global forum, championing strong and independent authorities. Key to this is ensuring that authorities can share cutting edge policy and enforcement experience*." Meanwhile, the ICO continues to work on their own cutting edge initiatives such as the regulatory sandbox.

It will certainly be another interesting and busy year in data privacy!

Rebecca Cousin
Partner

Regulator guidance

Key pieces of guidance published by the ICO and the EDPB in the second half of 2018 are included in the table below. The ICO also restructured their guidance in December 2018[1].

Key Regulator Guidance	
ICO	
Data protection if there is no Brexit deal	December 2018
Controllers and processors (see below)	December 2018
Contracts and liabilities	December 2018
Encryption	November 2018
Exemptions	September 2018
International transfers (see below)	August 2018
GDPR's seven key principles	June 2018
EDPB	
New annex to WP29 guidelines on accreditation (draft for public consultation - closes 1 February 2019)	December 2018
Guidelines on the territorial scope of the GDPR (draft for public consultation - closes 18 January 2018)	November 2018
Adopted opinions on Data Protection Impact Assessment lists	September and December 2018

ICO on controllers and processors

On 13 December 2018 the ICO published a suite of new guidance on controllers and processors, including expanding the contracts and controllers and processors sections of their Guide to the GDPR and publishing new detailed guidance on controllers and processors and contracts and liabilities.

Key takeaways from this guidance are:

- the ICO gives examples of the types of considerations controllers should have when assessing whether processors provide "sufficient guarantees" (in accordance with GDPR Article 28(1)). These include the extent to which processors comply with industry standards and whether processors have sufficient technical expertise to assist the controller;

[1] The ICO's Guide to the GDPR now sits within a broader Guide to Data Protection, which includes a new Introduction to Data Protection (covering basic concepts) as well as Guides to Law Enforcement Processing, Intelligence Services Processing and Key data protection themes.

- the clarification that a contract between a processor and sub-processor must include terms that "*offer an equivalent level of protection for the personal data as those that exist in the contract between the controller and the processor*", but "*do not need to exactly mirror*" those in the controller-processor contract. This is an important clarification on the wording in Article 28(4) that "*the same*" obligations must be imposed on the sub-processor as the processor;

- the ICO's recognition of the practical challenges for processors in complying with data deletion obligations at the end of processing contracts (in accordance with Article 28(3)(g)) and the suggestion that: "*[p]rovided appropriate safeguards are in place, such as the data being put immediately beyond use, it may be acceptable that the data is not deleted immediately if the retention period is appropriate and the data is subsequently deleted as soon as possible*";

- the clarification that the data protection fee is limited to being payable by controllers in the UK (that are not exempt); and

- the suggestion that joint controllers process the same set of personal data for the same purpose, implying that it is possible for controllers to process the same data set for different purposes and not be joint controllers (i.e. be controllers-in-common, although this terminology is not used in the guidance).

Brexit

Withdrawal Agreement rejected

As most will be aware, the **Withdrawal Agreement** which was agreed in principle between the UK and EU in November has been rejected by the UK Parliament. As the uncertainty around Brexit continues, we will be keeping a close eye on the impact of any proposed Brexit deal for the UK and EU data protection regimes.

No-deal planning

In December, the Government and ICO published a suite of guidance in preparation for a no-deal Brexit, seemingly in reaction to the ongoing political stalemate surrounding the Withdrawal Agreement.

On the 13 December the Department for Culture, Media and Sport (DCMS) published **guidance** on the amendments that would be made to UK data protection law in the event the UK leaves the EU without a deal on 29 March 2019[2]. This guidance confirms that following a no-deal Brexit, the GDPR will be retained in UK law by virtue of the EU (Withdrawal Act) 2018 (EUWA). It explains that to ensure the effective functioning of the UK data protection framework post-Brexit, the Government will make amendments to the GDPR and Data Protection Act 2018 by regulations made under the EUWA[3].

The key components of the no-deal framework highlighted by the guidance are:

- the UK will transitionally recognise all EEA states, EU and EEA institutions, and Gibraltar as providing an adequate level of protection for personal data, so data can continue to transfer freely from the UK to those destinations;

[2] This guidance followed their September 2018 technical notice on **data protection if there is no Brexit deal**, which we analysed in our article: **Deal or No Deal - UK Government issues technical notice on data protection.**
[3] The draft **Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019** were published at the beginning of January.

- where the EU has made an adequacy decision in respect of a country or territory prior to Brexit, the UK will preserve the effect of these decisions on a transitional basis, meaning that transfers from the UK to such "adequate countries" can continue uninterrupted, (this includes transfers to the US under the Privacy Shield);
- the UK will make provisions to recognise the SCCs previously issued by the EU Commission, so that they can continue to be used for international transfers from the UK, with the ICO being given power to issue new SCCs after Brexit;
- BCRs authorised by the ICO will continue to be recognised in UK law and the ICO will be able to continue to authorise new BCRs after Brexit[4];
- the UK's data protection framework will have extraterritorial effect post-Brexit and as such will apply to EU controllers or processors that are processing personal data about individuals in the UK in connection with offering them goods and services, or monitoring their behaviour; and
- controllers outside the UK, which are subject to the extraterritorial effect of the UK regime will be required to appoint a representative, subject to certain exceptions (replicating the existing GDPR Article 27).

On the same day the ICO published a **blog post** providing advice for organisations on data protection and Brexit. The post provided links to more detailed guidance for organisations on how to prepare for a no-deal Brexit, including a "**Six Steps to Take**" guide, detailed **guidance on the effects of leaving the EU without a withdrawal agreement**, **FAQs** and an **interactive guide** to SCCs for SMEs.

International transfers

ICO on international transfers

The ICO published expanded guidance on **international transfers** under the GDPR in August. The guidance provides a decision tree to help organisations assess: (i) whether a transfer of personal data out of the EEA is a 'restricted transfer' (i.e. subject to the GDPR requirements for international transfers); and (ii) the legal basis and mechanisms that may permit the transfer.

Interestingly, the guidance implies that there will not be a restricted transfer where: (i) the receiver is not a separate organisation or individual (i.e. it is a branch of the same organisation as the sender) or is employed by the same company as the sender; or (ii) the receiver is also subject to the GDPR. Protections such as the standard contractual clauses (SCCs) would therefore not be required in these two scenarios. The ICO acknowledges in its guidance that "*the EDPB is currently working on its guidance in relation to International Transfers*" and that the ICO will update its guide accordingly. Given the focus on international transfers over the last few years, it would be prudent for controllers to wait for the EDPB guidance to be published before relying extensively on the two exceptions mentioned above. International data transfers made in reliance on these exceptions without protections such as SCCs are also much more susceptible to challenge by privacy campaigners.

[4] It is likely but not yet certain that the EDPB will recognise existing BCRs as permitting transfers from EEA-to-UK group companies (with appropriate amendments made to recognise the UK's third country status) following a no-deal Brexit: see the ICO's **Six Steps** guidance.

Japan adequacy

In September the EU Commission **launched the procedure for the adoption of the EU-Japan adequacy decision.** At their **Fifth Plenary session** in December, the EDPB adopted an opinion on the adequacy decision as the next stage of the adoption process. However, according to the minutes of the Plenary, the EDPB expressed concerns about the protection for personal data provided by the Japanese regime. The EDPB has requested clarification regarding certain issues from the EU Commission which meant that the adoption of the adequacy decision was not completed last year as **previously anticipated**. The EDPB has emphasised that the EU-Japan adequacy decision is of paramount importance as it will set a precedent as the first post-GDPR adequacy decision.

EU-US Privacy Shield

The second annual review of the US Privacy Shield took place in October in Brussels, with senior officials from the US Government, the EU Commission and national data protection authorities participating. The EU Commission's **report** on the review (published on 19 December) states that the US continues to ensure an adequate level of protection for personal data transferred from the EU under the Privacy Shield. It notes that the US has taken steps to implement the EU Commission's recommendations in its **2017 report**. As a result the functioning of the framework has improved. The EU Commission has, however, called on the US to appoint a permanent Ombudsperson to replace the person who is currently acting.

Regulatory investigations and enforcement notices

Equifax Ltd

The ICO **fined** the credit reference agency Equifax Ltd £500,000 in September for failing to protect the personal information of up to 15 million UK individuals during a cyberattack in 2017. The ICO's investigation was carried out with the Financial Conduct Authority under the Data Protection Act 1998 (DPA98). The ICO found that Equifax had contravened 5 out of 8 of the DPA98 principles and gave the maximum penalty under the DPA98 regime. The ICO criticised Equifax on a very broad range of bases, including in relation to data retention and data security; the adequacy of its data processing contracts; and its failure to provide safeguards for international transfers. The scope of the ICO's review demonstrates how a data breach can expose all of an organisation's data protection policies and procedures to the regulator's focus.

ICO's Parliamentary report: data analytics in political campaigns

In November the ICO published a **report** to Parliament on its investigation into the use of data analytics in political campaigns. The investigation is the largest investigation ever by a data protection authority globally, and has involved the detailed review of over 30 organisations (from 172 initially identified), including political parties, data brokers and social media companies. The ICO has focused on the use of "invisible processing" in the context of political campaigns: it highlights the complex mechanisms and transfers that facilitate voter micro-targeting and the lack of transparency by the organisations involved. In light of its investigations, the ICO has recommended the introduction of a statutory code of practice on the use of data in campaigns and elections. A call for views on the proposal closed on the 21 December.

Key takeaways from the ICO's report that are relevant to all businesses:

- the ICO can expand their focus from one non-compliant company to review the practices of an entire industry; organisations can become subject to the ICO's scrutiny through no fault of their own;

- the ICO is focused on transparency; organisations should revisit their privacy notices to ensure they are GDPR compliant and, in particular, that they explain any surprising elements of their processing (which individuals would not reasonably expect) in a way individuals would understand;
- caution is required with respect to bought-in marketing lists: the ICO will want to see sufficient due diligence carried out on bought-in lists and their sellers to establish their pedigree and the reliability of any third-party consents obtained; and
- organisations need to be clear about the purposes for which they are processing data, and delete it (or put it beyond use[5]) when it is no longer required.

Facebook and Aggregate IQ

As part of the above investigation, in October, the **ICO fined** Facebook £500,000 (the maximum fine under the DPA98). However, the ICO stated that the fine would have been significantly higher under the GDPR. Facebook has since appealed. In the context of the same investigation, the ICO also issued their first post-GDPR enforcement notices (in **July** and **October**) against AggregateIQ, a Canadian company. For discussion of this enforcement notice and the implications for companies outside the EEA, see our publication: **The long arm of the law: EU privacy regulators enforcing the GDPR's extra-territorial reach**.

Cases

Wm Morrison Supermarkets PLC v Various Claimants

This case concerned Morrisons' appeal against last year's **High Court decision** that it was vicariously liable for the actions of an employee (S) who disclosed the personal information of around 100,000 colleagues on a data sharing website. Although Morrisons was itself not in breach of the DPA98, it was found vicariously liable for the actions of S, as there was sufficient connection between his employment and the wrongful conduct. This was despite the fact that the disclosure took place outside working hours from S' personal computer and S' motive being to harm his employer.

The Court's advice was for employers to insure against the risk of 'rogue' employees. In light of this, organisations should certainly ensure that no employee has access to information beyond what is strictly required for their role. For further analysis, see our November **Employment Bulletin**.

Lloyd v Google

This decision provided some welcome reassurance for data controllers that the UK courts will not blindly accept all claims for compensation by individuals. The full requirements of the Civil Procedure Rules still need to be met before such claims are allowed to progress. For further analysis of this decision, see our article **Data breach claims: a rebalancing by the English Courts**.

[5] See the ICO's latest guidance on data deletion by processors in its detailed guidance on **contracts and liabilities between controllers and processors**, discussed above.

Views from… California

One-year countdown to California's sweeping new privacy law: *Contributed by Allison Bender, Of Counsel and Megan Kayo, Associate, Wilson Sonsini Goodrich & Rosati*

The California Consumer Privacy Act (CCPA or Act) takes effect on 1 January 2020 with significant consequences for businesses that collect, disclose or sell the personal information of California residents. While there are differences, many have drawn comparisons between the CCPA and the European Union's General Data Protection Regulation (GDPR), which entered into effect 25 May 2018.

The CCPA greatly expands privacy rights for California residents, as the GDPR did for EU data subjects, although the rights granted are not synonymous. The CCPA specifically gives Californians the right to:

- know what personal information has been collected about them, whether that information is sold or disclosed and to whom;
- opt out of the sale of their personal information;
- access their personal information in a readily useable and transportable format;
- delete their personal information; and
- receive equal service at the same price, even if these rights are exercised.

"Personal information" as defined in the CCPA extends well beyond any prior U.S. privacy laws and is similarly broad to the GDPR's definition of personal data. It means "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." A "consumer" is defined as a natural person who is a California resident, which could be interpreted to include employees; "household" is not defined by the Act. The CCPA enumerates specific examples of "personal information" – including online IP address, account name, purchasing or consuming histories or tendencies, online browsing and search history, geolocation data, metadata and user profiles created from "inferences drawn" from consumer's preferences, characteristics, psychological trends, preferences, predisposition, behavior, attitudes, intelligence, abilities, and aptitudes. Unlike the GDPR, the CCPA excludes protected health information under the Health Insurance Portability and Accountability Act (HIPAA) and personal information collected by financial institutions under the Gramm-Leach-Bliley Act (GLBA), among other types of information.

"Businesses," as defined under the CCPA, that collect and/or determine the purposes and means of processing California residents' personal information can expect similar compliance obligations as "controllers" under the GDPR in many ways. This includes knowing how data flows to other parties and for what purpose; ensuring that consumer requests to exercise their rights under the CCPA are managed appropriately; and implementing reasonable security measures appropriate to the nature of the information. In addition, evoking but not replicating the GDPR concept of "processors," CCPA "service providers" of covered businesses must agree to abide by the requirements of the CCPA and assist in effectuating Californians' deletion requests, and CCPA "third parties" must not sell personal information about a consumer unless the consumer has received explicit notice and the opportunity to opt-out.

Unlike the GDPR, revenue thresholds and other criteria of the CCPA may affect when an entity is subject to the requirements of the CCPA. To be subject to the CCPA as a "business," an entity must be for-profit and meet one of the following three criteria: (i) annual gross revenue in excess of 25 million USD; (ii) buy or receive personal information of 50,000 or more California residents, households or devices; or (iii)

derive at least fifty percent of their annual revenue from selling consumers' personal information. A company that controls or is controlled by an entity that meets the criteria above and shares common branding is also considered a "business" under the CCPA. In practice, looking at the second criteria, a for-profit entity that collects website cookie data or does cross-device tracking may quickly exceed the combined total threshold of 50,000 consumer, households, or devices, in which case the CCPA applies regardless of revenue.

The CCPA, like the GDPR, authorizes regulatory fines and creates a limited private right of action with statutory damages for breaches. The California Attorney General may assess fines of $2,500 per any negligent violation and $7,500 per any intentional violation; private litigants may seek to recover data breach damages not less than $100 and not more than $750 per consumer per incident or actual damages, whichever is greater. In the United States, likely more so than in the EU under the GDPR, the CCPA may increase the risk of class action litigation following a data breach involving California residents. Given these potential enforcement and litigation risks coming into effect in 2020, businesses are likely to benefit from early compliance efforts.

2019 is the year to prepare for the CCPA.

Data Protection and Privacy at Slaughter and May

In our experience, data protection and privacy issues are relevant to all practice areas. Whether in the context of commercial transactions, M&A, global corporate and regulatory investigations or pension scheme arrangements, data protection is rarely a stand-alone issue.

All our fee-earners advise on data protection and privacy issues in their practice area. When faced with more complex and detailed data protection and privacy issues (including for example, complex global compliance strategies, cross-border transfers and data sharing schemes), our global data privacy hub provides the expert input that is needed. The hub is co headed by **Rebecca Cousin** and **Rob Sumroy** and, in our London office, comprises five partners.

If you would like further information please contact one of the team below, or your usual Slaughter and May contact.

Our other publications

We have published a series of articles on the GDPR and other data privacy areas. These can be accessed **here**.

Rob Sumroy
Partner
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Rebecca Cousin
Partner
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com

Richard Jeens
Partner
T +44 (0)20 7090 5281
E richard.jeens@slaughterandmay.com

Richard de Carle
Partner
T +44 (0)20 7090 3047
E richard.decarle@slaughterandmay.com

Duncan Blaikie
Partner
T +44 (0)20 7090 4275
E duncan.blaikie@slaughterandmay.com

Jordan Ellison (Brussels)
Partner
T +32 (0)2 737 9414
E jordan.ellison@slaughterandmay.com

Peter Lake (Hong Kong)
Partner
T +852 2901 7235
E peter.lake@slaughterandmay.com

Kevin Warburton (Hong Kong)
Counsel
T +852 2901 7331
E kevin.warburton@slaughterandmay.com