SLAUGHTER AND MAY

Data Protection and Privacy Newsletter

July 2018 / Issue 9

Selected legal and regulatory developments in data protection and privacy

Quick Links

This is the first edition of our newsletter since the long awaited GDPR became applicable. The 25 May came (and went) with much fanfare but most of our clients would admit they are not yet fully compliant. For the majority, GDPR compliance is a work in progress or as Elizabeth Denham acknowledged in her speech at the Data Protection Practitioners' Conference in April, the 25 May was "not the end. It is the beginning. This is a long haul journey".

Our experience shows that there are a number of common areas where difficulties are being encountered. We are regularly coming across challenges with data deletion as well as with the facilitation of individuals' rights. As part of this we have seen an uptick in the number of subject access requests we are being asked to advise on, although it is still early days. It will be interesting to see whether these will level out or remain part of the new post-GDPR landscape.

As expected, we have also seen an increase in the number of data breaches that we are assisting with under the GDPR mandatory notification regime. With the new regime, and the timeframe and sanctions, organisations are focussed on swift and correct decision making regarding notification. It is therefore unsurprising that more organisations are seeking external legal advice to ensure that they are taking the right steps.

We are retaining a close watching brief as Brexit progresses and continue to have conversations with our clients to monitor their areas of concern. We have been asked to join the ICO's Brexit panel with a small number of other law firms and will use the opportunity to relay the views of our clients and to gain a better understanding of the regulator's outlook and priorities for Brexit. If you would like to contribute to these Brexit conversations, please let us know.

Rebecca Cousin
Partner

GDPR application and related legal changes

On 25 May 2018 the long anticipated GDPR became applicable in all Member States and on 6 July 2018, the GDPR was incorporated into the EEA Agreement by the EEA Joint Committee. The GDPR will apply in the non-EU EEA states of Iceland, Lichtenstein and Norway once national legislation has been amended in accordance with the GDPR. This is expected to happen mid-July and will enable those countries' supervisory authorities to participate in the GDPR one stop shop and supervisory consistency mechanism.

Earlier in May a **corrigendum to the GDPR** had been published containing a number of minor corrections to the text. The most significant amendment was to the provision relating to data protection officers, which clarified that it was mandatory to appoint a data protection officer where the activities of a controller or processor consist of large scale processing of special categories of personal data or criminal conviction data. The text had previously included "and" in place of "or".

A number of other consequential changes also took place on the 25 May 2018 (in addition to the application of the DPA 2018), including the following:

European Data Protection Board

On 25 May 2018, the Article 29 Working Party ("A29WP") became the European Data Protection Board ("EDPB") as set out in the GDPR. Like the A29WP, the EDPB is made up of the head (or a representative) of each national data protection authority and the European Data Protection Supervisor. The European Commission can participate in meetings but cannot vote.

The EDPB is an independent body whose aim is to ensure the consistent application of the GDPR and the Law Enforcement Directive throughout the EU and to promote cooperation between national data protection authorities. Like the A29WP, the EDPB will provide guidance to clarify data protection law. It is also tasked with advising the European Commission on data protection issues and new legislation. In addition, the EDPB is required to issue binding decisions in relation to disputes between supervisory authorities and in cases where a supervisory authority does not follow the opinion of the EDPB (or does not request an opinion where required under the consistency mechanism.)

At the recent PL&B conference in Cambridge, Willem Debreuckelaere, President of the Belgian Autorité de la protection des données, explained that that the EDPB is currently working to produce new guidance on the territorial scope of the GDPR and on Data Protection Impact Assessments, both of which would be welcomed. He also explained that the EDPB have purposely not adopted the A29WP guidance on the e-Privacy Directive (2002/58/EC) because these guidelines need revisiting. He discussed that the EDPB may wait for the new e-Privacy Regulation before producing new guidelines, depending on how swiftly the e-Privacy Regulation progresses.

New funding structure for the ICO

The **Data Protection (Charges and Information) Regulations 2018** (the "Regulations") also came into force on 25 May 2018. Under the Regulations, data controllers must pay a fee to the Information Commissioner's Office ("ICO") unless they are exempt. The data protection fee replaces the requirement to notify under the Data Protection Act 1998. The fee payable is tiered according to an organisation's turnover and number of employees. There are three levels of fee ranging from £40 for micro organisations to £2,900 for large organisations. There are certain exemptions from the obligation to pay a fee, for example, where an organisation is only processing data for core businesses purposes.

Corporate groups will need to consider whether an exemption applies and what level of fee is payable in respect of each of their companies that is a controller established in the UK (or established outside the UK and processing personal data of individuals in the UK in certain circumstances).

Under the new regime the ICO has the power to serve monetary penalties of up to £4,350 (150% of the top tier fee) on those who fail to pay their data protection fee. Under the Data Protection Act 1998, failure to register could lead to a criminal conviction and unlimited fines.

The ICO have published a useful **guide to the data protection fee for controllers**.

ICO's powers of entry and inspection

The Data Protection Act 2018 ("DPA 2018") sets out the ICO's powers to enter and inspect business premises. These expanded powers are similar to those already held by UK and EU antitrust authorities, which are commonly referred to as 'dawn raid' powers. Failing to cooperate with, or to provide relevant information to, the ICO during such inspections can have serious consequences for both individuals and businesses. It is therefore important that businesses prepare for the possibility of on-notice and unannounced inspections by the ICO as this will reduce the immediate disruption and longer terms legal and business risks.

We will soon be publishing a full article on this subject in Privacy Law & Business.

Regulator guidance

Since our **last newsletter**, the ICO and the A29WP (as it was then known) have published a large amount of guidance in preparation for the incoming GDPR. Notably, the ICO has made substantial updates to its **Guide to the GDPR**. The ICO has also published an interactive tool on its website which aims to help controllers determine the right legal basis for their processing.

The table below lists some of the key pieces of detailed guidance published by the ICO and the A29WP since the beginning of the year[1].

Key Regulator Guidance	
ICO	
Children and the GDPR (finalised following consultation)	May 2018
Determining what is personal data	May 2018
Automated decision making and profiling	May 2018
Right to be informed	May 2018
Data protection impact assessments (finalised following consultation)	May 2018
Consent (finalised following consultation)	May 2018
Accountability and governance	April 2018
Security under the GDPR	April 2018
Business to business marketing under GDPR	April 2018
Legitimate interests as a lawful basis for processing	March 2018
Documentation obligations under the GDPR	January 2018

[1] Note: this is not a complete list of all guidance published by these regulators in 2018 (as there is too much for inclusion here). We do maintain a full list: let us know if you would find a copy useful.

A29WP / EDPB	
Guidelines on international data transfer derogations (finalised following consultation)	May 2018
Guidelines on consent (finalised following consultation)	April 2018
Guidelines on transparency (finalised following consultation)	April 2018
Guidelines on personal data breach notification (finalised following consultation)	February 2018
Guidelines on automated individual decision-making and profiling (finalised following consultation)	February 2018

EDPB on Transparency

The A29WP published its finalised guidelines on transparency on 14 April 2018 and the guidelines were endorsed by the EDPB on the 25 May 2018. The key takeaways from the guidance are:

- under the GDPR transparency is included as a fundamental principle, as part of the requirement for data to be processed lawfully and fairly.
- controllers should use their knowledge of the people they collect information about to produce communications that are tailored to their audience's level of understanding.
- layered website privacy policies, which contain a front-page summary with links through to greater detail, are the recommended way for privacy information to be delivered to data subjects in a digital context.
- in addition to layered notices, the entirety of the information addressed to data subjects should be available in one place/document which is easily accessible.
- children have an ongoing right to transparency throughout their relationship with a controller, regardless of consent to processing being given by their parent.

Data breaches: update

EDPB data breach guidelines finalised

Since our **last newsletter** the A29WP have updated their **data breach guidelines** and the guidelines have been endorsed by the EDPB. The finalised version contain the following notable changes:

- the controller is now only considered aware of a data breach when they are informed about the breach by their processor (rather than immediately on the processor becoming aware of it); and
- the A29WP (now EDPB) recommends that the processor informs the controller promptly of a breach occurring (rather than immediately).

These are welcome changes for both controllers and processors. The softening of the notification obligation on the processor (from immediately to promptly) will allow processors to carry out a modest amount of investigation into a potential data breach before they inform the controller. This should cut down the amount of 'false-alarm' notifications received by controllers and represents a more reasonable position for processors. However, prudent controllers are likely to still want to retain a time limit for their processors to inform them of a data breach, to ensure they can take meaningful steps to halt or mitigate a breach.

Cyber Security Breaches Survey 2018

The Department of Culture, Media and Sport published their latest **Cyber Breaches Survey 2018** at the end of April 2018. The headline figures from the survey are:

- 43% businesses surveyed experienced a cyber security breach or attack in the last 12 months;
- of the organisations that experienced breaches or attacks, 53% of businesses reported being impacted by them; and
- 74% businesses say that cyber security is a high priority for their organisation's senior management.

ICO's approach to enforcement: draft Regulatory Action Policy

Large scale data and cyber security breaches involving financial or sensitive information were identified in the ICO's **draft Regulatory Action Policy** (the "Policy") as one area of priority for ICO action in 2018-2019. Other areas of ICO priority include AI, big data and automated decision making, web and cross device tracking for marketing (including for political purposes) and privacy impacts for children (including Internet of Things connected toys). The ICO's draft Policy was published in early May 2018 for consultation and the consultation closed on 28 June 2018. At the recent PL&B conference in Cambridge, an ICO spokesperson commented that the ICO hopes to publish the final version over the summer.

In launching the Policy, James Dipple-Johnstone, the Deputy Commissioner reiterated that the ICO will "*target our most significant powers on repeated, wilful or serious failures to take proper steps to protect personal data and deliver information rights.*" In this light, the Policy sets out a list of the factors that the ICO will consider in deciding how to respond to breaches of data protection law. Alongside factors relating to the more factual circumstances of the breach, the Policy includes the following factors relating to the broader attitude and conduct of the controller:

- whether the attitude and conduct of the organisation concerned suggests an intentional or negligent approach to compliance;
- whether relevant advice or guidance from the ICO has been followed; and
- the manner in which the breach or issue became known to the ICO and, if relevant, to what extent the relevant individual or organisation notified the ICO of the breach or issue.

The ICO has recently published a **progress report** and a **partner report** in connection with its investigation into the use of data analytics in political campaigns. These documents provide a useful insight into the approach that they ICO will take in high profile cases involving large-scale processing of personal data, in particular through the use of new technologies and data analytics.

International transfers: update

Adequacy: EU-Japan agreement

Japan and the EU successfully concluded their talks on mutual adequacy on 17 July 2018. The parties have committed to completing the relevant internal procedures to give effect to their adequacy findings by autumn 2018. When concluded, the mutual adequacy findings will facilitate the uninhibited transfer of data between the EU and Japan. According to the European Commission's **press release** the adequacy agreement covers personal data exchanged for commercial purposes as well as the exchange of data for law enforcement purposes.

Privacy shield

On 5 July 2018, the European Parliament voted in favour of a non-binding **resolution** that calls on the European Commission to suspend the Privacy Shield from 1 September 2018. The resolution states that the current Privacy Shield arrangement does not provide the adequate level of protection required by EU data protection law and the EU Charter. The deficiencies identified in the resolution include the lack of regulatory supervision of US companies' after self-certification and the complexity of the recourse procedures for EU citizens as well as the deficiencies in the Privacy Shield highlighted by the Cambridge Analytica/Facebook case. The resolution also highlights the US's recent adoption of the Clarifying Lawful Overseas Use of Data ("CLOUD") Act as a source of concern. The CLOUD Act extends the abilities of American and foreign law enforcement agencies to access individuals' data across international borders without the use of mutual legal assistance instruments which provide safeguards.

The European Parliament's resolution followed a vote by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs on the 11 June 2018 in favour of a **motion** that the Privacy Shield in its current form does not provide the adequate level of protection required by EU data protection law and the EU Charter.

Standard Contractual Clauses: Schrems case update

The Irish High Court has now **published** the 11 questions that it is referring to the CJEU in the Schrems-Facebook case. The questions to be considered are broad and include consideration of whether international transfers under the Standard Contractual Clauses violate Articles 7 and 8 of the EU Charter (respect for private and family life, and protection of personal data) as well as potentially bringing into question the validity of the Privacy Shield.

At the beginning of May the Irish High Court rejected an attempt by Facebook to delay the reference of the questions to the CJEU. However, the Irish press have reported that, on 17 July, the Irish Supreme Court will hear Facebook's application for permission to appeal the High Court judge's decision to refer the questions to the CJEU (which is essentially a 'leapfrog' procedure).

Brexit

On 23 May 2018, the UK government published a **presentation** on the framework for the future UK-EU partnership in data protection, for discussion between the UK and EU negotiating teams. The presentation proposes a new agreement between the EU and UK which goes beyond standard adequacy. The proposal suggests that the agreement should: (i) maintain the free unhindered flow of personal data between the EU and UK; (ii) provide for continued regulatory co-operation and consistent enforcement through an appropriate ongoing role for the ICO on the EDPB; (iii) ensure UK businesses and consumers are effectively represented under the EU's new one stop shop mechanism for resolving data protection disputes; and (iv) include amendment, dispute resolution and termination provisions.

However, on the 26 May 2018 Michel Barnier rejected a number of the UK's proposals in a **speech** given at the 28th Congress of the International Federation for European Law. He stated that the only option for the EU to protect personal data is through an adequacy decision (rather than a negotiated agreement) and explained that the EU would not abandon its decision making autonomy by allowing the ICO to participate in the EDPB or the one stop shop post-Brexit. On 7 June 2018 the UK government published a **technical note** setting out the benefits of a new data protection agreement which seemed to try to address some of the concerns Michel Barnier raised in his 26 May 2018 speech, particularly in relation to the EU's decision-making autonomy.

The UK government's controversial 12 July 2018 white paper on **the future relationship between the United Kingdom and the European Union** (the "White Paper") contains a specific section dealing with data protection. This largely restates the government's position as set out in the May presentation. It reasserts that the UK will be seeking a data protection agreement with the EU that goes beyond adequacy and that there should be continued close co-operation between the ICO and the European data protection authorities. Notably, however, it does not specifically make reference to the ICO's continued membership of the EDPB after Brexit which may demonstrate a slight shift in the government's approach.

The White Paper states that the UK is ready to begin preliminary discussions with the European Commission in relation to an adequacy decision in order for a data protection agreement to be in place by the end of the transition period at the latest[2]. It is not clear whether the European Commission will be open to such discussions at this stage.

ICO regulatory co-operation

The ICO has been co-operating with other UK regulators to provide specific guidance on the GDPR.

ICO/FCA joint update

In February the FCA and ICO published a **joint update** on the GDPR. The key messages from the update were:

- financial services firms must comply with the GDPR;
- the FCA and ICO believe that the GDPR does not impose requirements which are incompatible with the rules in the FCA Handbook;
- compliance with the GDPR is now a board level responsibility and firms must be able to evidence the steps they have taken to comply; and
- although the ICO will regulate the GDPR, the FCA will take compliance with the GDPR rules into consideration under their rules.

ICO/NCSC GDPR Security Outcomes

On the 18 May 2018 the National Cyber Security Centre ("NCSC") published guidance on **GDPR Security Outcomes** that had been developed with the ICO. The guidance describes a set of technical security outcomes that are considered "appropriate" to prevent personal data being accidentally or deliberately compromised, as required under the GDPR. The outcomes focus on four areas: management of security risk; protection of personal data against cyber-attack; detection of security events; and minimisation of the impact of a personal data breach.

Delay to e-Privacy Regulation

In March the UK government confirmed that the e-Privacy Regulation was delayed and would not be ready to apply from 25 May 2018 to coincide with the GDPR, as had been intended. The government explained that the EU Council was aiming for a General Approach (an informal agreement within the Council) regarding the e-Privacy Regulation by the end of June 2018.

On 25 May 2018 the President of the European Council published a **progress report** on the e-Privacy Regulation, which describes the current state of play in the Council and refers to a number of compromise texts that have been issued by the Presidency this year. Following that, the EDPB issued a **statement** at the beginning of June calling on the European Commission, Parliament and Council to work together to ensure a swift adoption of the new e-Privacy Regulation.

At the recent PL&B conference, Elizabeth Stafford from the Department for Culture, Media and Sport described some of the issues being discussed by the European Council in relation to the e-Privacy Regulation. She referred in particular to the interaction between the e-Privacy Regulation and the GDPR and held that the e-Privacy Regulation is intended to prevail over the GDPR where it provides more specific rules. She gave the example that Article 6 of the e-Privacy Regulation is more detailed than the GDPR and therefore should prevail. Conversely, she explained, the GDPR provisions relating to individuals' rights and international transfers should prevail.

[2] This is in line with a recommendation from the House of Common's Brexit Committee (in their 7 July 2018 report) that the government should seek to initiate the adequacy process without delay to avoid a gap in legal provision for UK-EU data transfers after December 2020.

Views from… Canada

Contribution by Wendy Mee, Partner, and Catherine Beagan Flood, Partner, Blake, Cassels & Graydon LLP

Canada's new mandatory data breach reporting regime

Amendments to Canada's federal Personal Information Protection and Electronic Documents Act ("PIPEDA") in 2015 (via the Digital Privacy Act) introduced provisions that created a federal mandatory breach reporting regime for Canada's private sector. However, the effective date of those provisions was delayed pending regulations setting out prescribed requirements for breach reporting. The final version of the regulations, the Breach of Security Safeguards Regulations ("Regulations"), were made on 26 March 2018 and published on 18 April 2018. The Regulations set out the requirements for mandatory breach reporting and bring the new regime into force on 1 November 2018. Currently, Alberta is the only province that requires reporting of private sector data breaches outside the healthcare context.

Under the new regime, PIPEDA will require breach notifications to be made where an organisation experiences a "breach of security safeguards" involving personal information under its control and it is reasonable in the circumstances to believe that the breach poses a "real risk of significant harm" to affected individuals. In that circumstance the organisation must: (i) report the breach to the Privacy Commissioner of Canada ("Commissioner"); (ii) notify affected individuals; and (iii) notify government institutions, parts of government institutions or other organisations if the organisation believes that the institution or other organisation may be able to reduce or mitigate the risk of harm to the affected individuals. It should also be noted that in contrast with many U.S. breach reporting requirements, the definition of "personal information" in PIPEDA is very broad, and the Canadian definition of harm encompasses non-economic harm. The Canadian definition of harm is more comparable to the GDPR concept of damage, which encompasses non-material damage such as damage to reputation.

The notifications to both the Commissioner and to individuals must be made as soon as feasible after the organisation determines that the breach has occurred. The Regulations set out the form and manner in which the notifications must be made, as well as the information that must be included in them.

PIPEDA also requires organisations to keep and maintain a record of all breaches of security safeguards under the organisation's control, even those that do not meet the harm threshold for reporting. An organisation that knowingly fails to report or maintain records of a breach as required by PIPEDA will be guilty of an offence punishable by fines of up to C$100,000.

Data Protection and Privacy at Slaughter and May

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 due diligence in a possible takeover, employment issues, litigation, outsourcing, global corporate and regulatory investigations or public sector data sharing schemes, data protection is rarely a stand-alone issue. All our fee-earners are trained to spot and advise on data protection and privacy issues. 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), we draw on our network of specialist data protection and privacy advisers from across the firm, including our overseas offices. These individuals have particular knowledge and experience of data protection and privacy issues, but they each sit within their distinct practice areas and thus have additional expertise and skills to bring to the table. Our global network of advisers is co-headed by **Rebecca Cousin** and **Rob Sumroy** and is supported in our London, Brussels and Hong Kong offices by a number of data protection and privacy partners.

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)
Associate
T +852 2901 7331
E kevin.warburton@slaughterandmay.com