SLAUGHTER AND MAY

Data Protection and Privacy Newsletter

July 2017 / Issue 7

Selected legal and regulatory developments in data protection and privacy

Quick Links

This newsletter provides a round-up of various developments in data protection and privacy over the last 6 months or so, which are worthy of note but which have not made it into one of our other briefings.

Some, but not all, of the items relate to companies' and regulators' preparations for the General Data Protection Regulation (GDPR). But there have been developments in other areas too, such as in respect of subject access requests and direct marketing. In addition, as is our custom, we have a contribution from one of our relationship firms - this time from Lenz & Staehelin in Switzerland.

Many companies are now well underway with their GDPR compliance programmes. Others, whose processing may be less complex, have started more recently. What is clear is that if a company has not yet started its programme, there is no time like the present - a lot can be achieved before the GDPR comes into force. There is some information at the end of this newsletter about how we are helping clients on GDPR compliance, starting with a no obligation and no cost kick-off meeting.

If you would like any further information on any of the items covered, or would like to discuss any other data privacy matter, please contact me or one of our Data Protection and Privacy team (our details are at the end of this newsletter), or your usual Slaughter and May contact.

Rebecca Cousin
Partner

Preparing for the GDPR – UK Data Protection Bill

While the GDPR does not require full transposition into national law in the UK, there are certain aspects for which national law will be required. The UK government has announced that any aspects where national law is required will be included in its proposed Data Protection Bill which was referred to in this year's Queen's Speech.

Derogations

One area where new law is needed is where there are national discretions or derogations in the GDPR that the UK intends to exercise. In April 2017, the Department for Culture, Media and Sport (DCMS) called for views on these. The consultation period ended in May and a response is awaited. For some

sectors, the derogations are particularly important given that the GDPR does not include the extra grounds for processing sensitive personal data that are currently contained in various statutory instruments, such as ones relevant to insurers under the Data Protection (Processing of Sensitive Data) Order 2000.

ICO powers

Another area where national law is expected is in regard to the powers and sanctions available to the Information Commissioner's Office (ICO). However, it is possible that the provisions of the Data Protection Bill may extend further than what is required by the GDPR.

In its response to DCMS's call for views on national derogations, the ICO argued for the introduction of a new criminal offence of intentionally reversing or circumventing de-identification measures, or being reckless as to whether actions result in re-identification. This is in light of growing concerns about the risk that individuals may be re-identified from apparently or purportedly anonymised data sets, particularly in big data initiatives and healthcare. Prior to the 2017 General Election, the UK Government had previously expressed its intention to introduce stronger sanctions for deliberate and negligent re-identification of anonymised data. It therefore seems likely that such an offence will find a place in the Data Protection Bill.

GDPR guidance from the Article 29 Working Party

In April 2017, the Article 29 Working Party (WP29) adopted final versions of its GDPR guidelines on the right to data portability, guidelines for identifying a controller or processor's lead supervisory authority and guidelines on Data Protection Officers. The WP29 also published draft guidelines on Data Protection Impact Assessments and determining whether processing is "likely to result in a high risk" (under Article 35 of the GDPR). The final version of this is expected in October 2017.

Other guidance from the WP29 is now expected to be published by December 2017. Anticipated materials include guidance on consent, transparency and data breach notification (for which the ICO is the lead national authority). With this timing, there is a risk that organisations will not have sufficient time to revisit their own analysis or adapt policies or processes where necessary once the guidance is available. The timing will also affect publication of any UK guidance from the ICO on the same topic, in particular the ICO's consent guidance as discussed below.

GDPR guidance from the ICO

The ICO has also published guidance on the GDPR, but it has so far been less prolific that the WP29.

One key aspect of the ICO draft guidance on consent (published in March 2017) is it provides that, where consent is the legal basis for processing, third parties must be named in privacy notices and that even precisely named categories are not acceptable. However, Articles 13, 14 and 15 of the GDPR allow an organisation to set out categories of third parties as an alternative to a name. Arguably, setting out categories of third parties is more transparent than providing the name of a third party (as a company name may not indicate a third party's activities). The ICO has recently stated that the final version of this guidance will not be available until after the WP29 has released its guidance on the same topic. As noted above, the WP29 guidance is expected by December 2017. In the meantime, the ICO plans to publish a summary of the responses to its consultation.

The ICO also published a discussion paper on profiling in April 2017. This was intended to help inform its approach to the WP29's guidelines on profiling, expected by December 2017, and for which the ICO is the lead national authority.

Data processing in the workplace

While not officially designated as GDPR guidance, the WP29 published in June 2017 an opinion on data processing in the workplace. This was stated as complementing its existing 2001 opinion on the processing of personal data in the employment context and its 2002 Working Document on the surveillance of electronic communications in the workplace. While primarily concerned with the position under the existing regime, the new opinion also looks ahead to the GDPR. It recommends, among other things, that data protection impact assessments be conducted and that privacy by design and default be adopted when introducing new technology for use by employees. More generally, the opinion provides practical guidance for employers in relation to new technologies and recruitment activities (such as screening candidates' social media profiles).

Challenges to international transfers

Challenges to international transfers continue to be a concern in the first half of 2017. We discuss the wider implications of such challenges on free trade in our article **Data protection or protectionism by the back door?**

Brexit

In light of Brexit, a critical issue is whether the UK will obtain an adequacy finding from the European Commission either at all or at the point that the UK leaves the EU. Without this, the UK will be a non-whitelisted third country. An adequacy finding would provide the most straightforward and comprehensive mechanism for organisations to enable data transfers from the EU to the UK. Indeed, key Parliamentary committees in the House of Commons and the House of Lords have recommended that the UK Government seek an adequacy decision to facilitate future EU-UK data transfers. However, the UK Government has declined to confirm whether it will do so on the grounds that any public statement on the topic may fetter its negotiation position.

Model clauses

Since the previous issue of the **Data Protection and Privacy Newsletter**, the Irish High Court has heard the challenge by Maximillian Schrems to the EU standard contractual clauses ("model clauses") and has reserved judgment. A key matter it must decide is whether a reference should be made to the Court of Justice of the European Union (CJEU) concerning the validity of model clauses and, if so, what questions to refer. While the Irish High Court has considered the model clauses in so far as they relate to transfers from the EU to the US, any doubts or questions about their validity may have implications for transfers to other countries.

The judgement of the Irish High Court or any reference it makes to the CJEU will therefore be of great interest to many organisations.

E-Privacy reform

In January 2017, the European Commission announced a further step in the reform of EU data protection law when it published a draft E-Privacy Regulation (Draft Regulation) to replace the Privacy and Electronic Communications Directive (PECD). The PECD governs, among other things, direct marketing via electronic means, cookies and mandatory data breach notification duties on communications providers. The PECD is implemented in the UK through the Privacy and Electronic Communications Regulations 2003 (PECR).

As a Regulation, the Draft Regulation would apply directly to Member States (including the UK, if the UK has not exited the EU by the date the Draft Regulation applies), which would help achieve better harmonisation and lower compliance costs for pan European businesses. Its scope is also extended to

over-the-top service providers (such as instant messaging or VOIP). Other changes include those reflecting more alignment with the GDPR such as on extra-territoriality.

Fines of up to 4% of annual world-wide turnover may be imposed for breach, but there is concern that the current drafting leaves it open for an organisation to be fined under both the Draft Regulation and the GDPR for the same breach. Given the mandatory breach notification regime under the GDPR, the Draft Regulation does not include separate provision for this. This means that the GDPR's 72 hour deadline for notification will apply to telecommunications providers in place of the current 24 hour deadline under PECR.

The European Commission intends the Draft Regulation to take effect at the same time as the GDPR, on 25 May 2018. However, this is an ambitious timetable without a proposed transition period and is therefore likely to be challenging for many organisations if the European Commission meets its own timetable.

Direct marketing

Digital Economy Act

The Digital Economy Act 2017 received Royal Assent at the end of April 2017 during the wash-up period before Parliament dissolved ahead of the General Election. The Act will introduce new provisions relevant to direct marketing, which came into force at the end of June.

These provisions require the ICO to prepare a statutory code of practice for direct marketing. There is existing ICO guidance on direct marketing but the status of the new code of practice will be different as it will be admissible as evidence in any legal proceedings against an organisation (not only proceedings under the Data Protection Act 1998 (DPA)).

The new code of practice will cover practical guidance in accordance with the DPA and PECR, and such other guidance as the ICO considers appropriate to promote 'good practice' in direct marketing. 'Good practice' is defined to mean such practice as appears to the ICO to be desirable, having regard to the interest of data subjects among others. This wide definition means that the new code of practice has the potential to be more restrictive than what is otherwise permitted under law.

The ICO will be required to consult with key stakeholders on this code as it considers appropriate, including trade associations.

Draft E-Privacy Regulation

The Draft Regulation (for a general discussion on this, see above) broadly continues the existing rules on direct marketing which requires organisations to obtain a prior opt in consent. However, it will raise the bar for what is considered valid consent, as it imports the GDPR's definition of consent.

Usefully, the Draft Regulation continues to provide for the 'soft opt-in' which allows an organisation to e-mail its existing customers about similar products or services subject to a right to object being included when the data was collected and in each subsequent communication.

Recent ICO action

In March 2017, the ICO fined UK-based airline Flybe £70,000 after the company sent more than three million emails to individuals who had previously stated that they did not want to receive marketing emails from Flybe. The emails advised the recipients to update their marketing preferences and amend any out-of-date information.

Also in March 2017, the ICO fined Honda £13,000 after Honda sent emails to individuals in order to clarify their marketing preferences, where individuals had previously agreed to some form of direct marketing but it was unclear what their actual preference was (due to a design failure in the database), or where

Honda had no marketing preference details. Honda argued that the emails were service emails, not marketing emails, and that they had been sent with the intention of ensuring compliance with data protection principles on retention and accuracy of personal data they held.

In July 2017, the ICO fined price comparison website Moneysupermarket.com £80,000 for sending over seven million emails to customers updating them with new terms and conditions. Every recipient had previously chosen to opt out of direct marketing. The email included a section asking the recipient if they would like to reconsider their opt out.

All three actions were taken by the ICO on the basis that organisations cannot email an individual to ask for consent to future marketing messages. Such an email is itself deemed to be direct marketing and would therefore be subject to the direct marketing rules in PECR. Accordingly, legitimate service emails on other matters should not be used to ask individuals to reconsider their marketing preferences where they have previously opted out or where there may be doubt as to their preference.

ICO guidance on subject access requests

In June 2017, the ICO updated its code of practice on Subject Access Requests (SARs). The changes reflect the judgments handed down earlier this year by the Court of Appeal in the case of Dawson-Damer and Taylor Wessing LLP[1] and joined cases of Ittihadieh/Deer and Oxford University[2]. The Court of Appeal's judgments had been eagerly awaited and were disappointing from the perspective of data controllers and particularly employers who face SARs from employees who are contemplating or actively pursuing litigation against them.

Collateral purpose

The Court of Appeal held that there is nothing in the DPA or the underlying Data Protection Directive which limits the purpose for which a data subject may request his data, or (conversely) provides data controllers with the option of not providing data based solely on the requester's purpose.

The SAR code of practice has been reflected to amend this but recognises the court's wide discretion as to whether to order compliance with the SAR. The guidance sets out the range of factors that the Court of Appeal suggested the court may wish to take into account, including:

- the nature and gravity of the data controller's breach of its SAR obligations;
- the general principle of proportionality;
- balancing the fundamental right of subject access with the interests of the data controller;
- prejudice to the individual's rights;
- whether there is an abuse of process or a conflict of interest; and
- whether there is a more appropriate route to disclosure.

The last of these factors in particular gives some hope to data controllers as to the ability to limit the scope of responding to a SAR, but the ICO points out that these are not factors affecting the obligation of the data controller to comply with the SAR but go to whether the court will enforce compliance.

[1] Dawson-Damer and others v Taylor Wessing LLP [2017] EWCA Civ 74

[2] Ittihadieh v 5-11 Cheyne Gardens RTM Company Ltd and others [2017] EWCA Civ 121, joined with Deer v Oxford University

Disproportionate effort exemption

The Court of Appeal held that the burden of proving the "disproportionate effort" exemption under Section 8(2)(a) of the DPA lies on the data controller. The judgment suggests this will be a heavy burden, given the substantial public policy reasons for giving people control over the data maintained about them. The court also made the point that most data controllers can be expected to know of their obligations to comply with SARs, and to have designed their systems accordingly to enable them to make most searches for SAR purposes.

Again, the SAR code of practice has been amended to reflect the judgments and, in particular, notes that:

- the disproportionate effort exemption cannot be used to justify a blanket refusal to respond to a SAR as the data controller must do what is proportionate in the circumstances;
- the data controller may take into account difficulties that arise whilst seeking to comply with the SAR, such as in finding the requested information;
- the ICO expects data controllers to evaluate the particular circumstances of a SAR, balancing any difficulties involved in complying against the benefits the information might bring to the data subject, whilst bearing in mind the fundamental nature of the right of access;
- the burden of proof is on data controller to show that it has taken all reasonable steps to comply with the SAR and that it would be disproportionate to take further steps;
- it is good practice for the data controller to engage with the data subject, having an open conversation with the individual about the information they require; and
- if the ICO receives a complaint about a SAR from a data subject, it may take into account the data controller's readiness to engage with the applicant and balance this against the benefit and importance of the information to them, as well as taking into account their level of co-operation with the data controller.

Whilst the guidance relates to the DPA and not the GDPR, many aspects will continue to be relevant. For further details see our briefing **What do employers in the UK need to know about the General Data Protection Regulation (GDPR) from an employment perspective?**

Views from...Switzerland: New privacy shield agreement facilitates cross-border data transfer from Switzerland to USA

Contribution by Lukas Morscher, Partner, Head of TMT and Outsourcing, and Stefan Bürge, Associate, Lenz & Staehelin

Swiss-US Privacy Shield

Following the decision of the CJEU that the US-EU Safe Harbour Framework did not provide adequate protection for the transfer of personal data abroad, the Federal Data Protection and Information Commissioner (FDPIC) declared that the US-Swiss Safe Harbour Framework could also no longer be considered to provide adequate protection for the transfer of personal data from Switzerland to the US.

This led to the negotiation of a new agreement on cross-border data transfer from Switzerland to the US which generally encompasses the same requirements as the EU-US Privacy Shield. The Swiss-US Privacy Shield framework became fully operational on 12 April 2017 and, as of that date, US organisations processing personal data have been able to self-certify for the Swiss-US Privacy Shield and thus commit to comply with the new framework. As a result, Swiss companies are able to transfer personal data to self-certified US business partners without the need to procure the consent of each data subject or to put additional measures in place.

By mid-June 2017, 379 organisations had self-certified for the Swiss-US Privacy Shield (compared to 2198 organisations who have self-certified for the EU-US Privacy Shield).

As is the case with the EU-US Privacy Shield, the Swiss-US Privacy Shield imposes tougher obligations on US companies than under the previous regime.

US-based organisations which are already certified under the EU-US Privacy Shield separately need to self-certify under the Swiss-US Privacy Shield if they transfer personal data from Switzerland to the US. Such extension of the EU-US self-certification can be easily effected through the DOC's online portal.[3]

Switzerland based organisations transferring personal data to the US should review the corresponding agreements and assess whether they relied on the now terminated US-Swiss Safe Harbour. If so, the respective agreements must be amended to either rely on the Swiss-US Privacy Shield or include alternative safeguards.

Rather than self-certify to the Swiss-US Privacy Shield, US and Switzerland based organisations may still wish to rely on alternative safeguards such as implementing (standard) contractual clauses or binding corporate rules. Based on first practical experience, alternative safeguards may even be preferable in some cases because:

- implementing the Swiss-US Privacy Shield may be a cumbersome process for organisations which have not already self-certified to the EU-US Privacy Shield; and
- the long-term viability of the Swiss-US Privacy Shield remains uncertain. The similar EU-US Privacy Shield has already been challenged before the CJEU and the FDPIC has reserved the right to re-evaluate the adequacy of protection provided by the Swiss-US Privacy Shield.

Reform of Swiss data protection law

Swiss data protection law is currently being revised. Expected amendments include extended information and notification duties (e.g. regarding data breaches), the obligation to conduct data privacy impact assessments in certain cases and fines of up to CHF 500,000 in case of non-compliance.

The consultation on the preliminary draft ended on 4 April 2017. The revised Swiss DPA, once finalised, is expected to enter into force in 2018.

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

[3] See **www.privacyshield.gov**

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. That network of advisers is co-headed by **Rob Sumroy** and **Rebecca Cousin** and is supported in our London office by data protection and privacy partners **Richard Jeens**, **Richard de Carle** and **Duncan Blaikie**, and data protection and privacy professional support lawyer Cindy Knott.

How we can help you with GDPR

No company is the same as another and so each will need differing levels and types of support with their GDPR compliance programme. We tailor the scope and nature of our support to suit the individual client's needs, taking into account the data protection and privacy laws in all relevant jurisdictions. A few examples of the type of support we can offer you with your GDPR compliance programme include assisting you in **preparing or reviewing your GDPR programme** (e.g. gap analysis, advice on different approaches or areas that may have been missed and market practice), **answering ad hoc queries on your GDPR programme**, **assisting with one-off projects** to support certain parts of your GDPR programme and providing **training**.

We would be very happy to meet with you to discuss further (on a no charge basis) the support we can offer you.

Rob Sumroy
T +44 (0)207 090 4032
E rob.sumroy@slaughterandmay.com

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

Richard Jeens
T +44 (0)207 090 5281
E richard.jeens@slaughterandmay.com

Richard De Carle
T +44 (0)207 090 3047
E richard.decarle@slaughterandmay.com

Duncan Blaikie
T +44 (0)207 090 4275
E duncan.blaikie@slaughterandmay.com