SLAUGHTER AND MAY

Data Protection and Privacy Newsletter

January 2018 / Issue 8

Selected legal and regulatory developments in data protection and privacy

Quick Links

Since the **previous edition** of our Newsletter, data privacy issues have continued to make headlines (or made for work in avoiding them!). Nothing is more likely to splash a company across the front pages than a data breach, and we have certainly seen a good number of those both through our work for clients and in the news.

At the end of last year we hosted our annual Data Privacy Forum with data breach being one of the topics up for discussion. Emma Bate, General Counsel of the ICO, gave the key note speech at our Forum sharing insights into the current work and thinking of the ICO, including their pilot on notification of data breaches. Other topics discussed were operationalising the GDPR, demonstrating accountability and compliance and data processor contracts.

As with last year's Forum, we asked attendees what was the biggest challenge to their organisation's GDPR compliance. The results were interesting in of themselves, but even more so in comparison to last year. The two biggest changes were budgetary constraints increased as an issue whilst lack of practical preparation reduced. This no doubt reflects the amount of work many organisations have undertaken, and therefore the costs incurred to date.

We will be issuing a publication covering some of the points raised in the breach session shortly whilst points from the processor session were picked up in the GDPR client training we ran in December. If you would like further details on any of the Forum discussions, please let us know.

Even for companies who started preparing for the GDPR some time ago, it is going to be a sprint to the finish for many, with 71% of attendees at our Forum saying (obviously anonymously) that their organisation would not be fully compliant on 25 May 2018. An interesting, if not surprising, response. From the way my phone has been ringing, GDPR planning seems to be a New Year's Resolution for many organisations and I would certainly encourage anyone who has not yet started to pick up the baton now.

It is certainly interesting (and busy!) times in the data privacy world.

Rebecca Cousin
Partner

Data Protection Bill

First introduced to the House of Lords on 13 September 2017, the Data Protection Bill ("the Bill") will repeal the Data Protection Act 1998 and implements various exemptions and derogations permitted under the GDPR. In the UK, the GDPR therefore needs to be read alongside this legislation in order to fully assess the legal position.

In September 2017 Rebecca Cousin joined a panel of data privacy legal experts at a round table organised by the Department for Digital, Culture, Media and Sport and the ICO, as part of the government consultation on the Data Protection Bill. This was an opportunity to provide headline comments and proved a useful forum for passing on the views of ourselves and our clients on the approach taken in various areas. Some of these areas have since been addressed in the Government's proposed amendments to the Bill, which were incorporated into the House of Lords' Committee amendments.

The Bill has been going through the House of Lords and was updated with amendments on 22 November 2017 after the conclusion of the House of Lords committee stage. The House of Lords had a further opportunity to examine and make amendments at the report stage which completed on 10 January 2018. A third and final reading of the Bill in the House of Lords started on 17 January 2018.

Regulator Guidance on the GDPR

*Status of ICO and Article 29 Working Party ("*A29WP") *Guidance*

Regulators have been busy over the last six months publishing guidance on various topics. We have listed below the key guidance issued by the A29WP and the ICO during this period and also highlighted the guidance that is expected.

Topic	Date of issue	Status
A29WP		
Data breach notification (see our article)	3 October 2017	Consultation on draft guidelines has closed
Administrative fines	3 October 2017	Adopted guidelines
Data Protection Impact Assessment	4 October 2017	Revised and adopted guidelines
Profiling and automated decision making	17 October 2017	Consultation on draft guidelines has closed
Consent (see summary below)	28 November 2017	Open for comments until 23 January 2018
Transparency	28 November 2017	Open for comments until 23 January 2018
ICO		
Contracts and liabilities between controllers and processors	13 September 2017	Consultation on draft guidance has closed
Consent	21 November 2017	Updated draft guidance published. Final guidance is expected once the A29WP guidance is finalised
Children's data (see summary below)	21 December 2017	Public consultation until 28 February 2018
Legitimate interest and other lawful grounds for processing		Expected later this year

A29WP: consent

These new guidelines expand upon earlier references and opinions on consent by the A29WP.

Key takeaways from the guidance include:

- the increasing onus on controllers to demonstrate the validity of consent obtained (although how they demonstrate it is up to them);
- the strict and potentially wider scope of the wording in the "conditionality" rule when determining whether consent is freely given;
- no specific time limit for consent, although the A29WP provide that best practice is that the consent should be refreshed at regular intervals; and
- that when relying on consent it will not be possible to switch to another lawful basis if the consent is deemed to be invalid or withdrawn.

ICO: processing children's data

Key takeaways from this draft guidance are that:

- children explicitly warrant specific protection when collecting their personal data for marketing purposes or creating personality or user profiles;
- given the provisions under the Bill that only children aged 13 or over are able to provide consent in relation to an online service, organisations relying on consent will need to verify that the individual satisfies this;
- if a child is under the age of 13, organisations will need to make reasonable efforts to verify that the provider of consent was the holder of parental responsibility for the child.

e-Privacy Regulation

We discussed the proposed e-Privacy Regulation in the **previous edition** of our Newsletter. Since then there have not been as many developments as one might have expected. As noted at that time, the European Commission's intention for it to take effect on 25 May 2018, alongside the GDPR, was ambitious. Whilst nothing has been said formally, from what we have heard, and the progress so far, this now seems improbable.

Instead we expect that the text will be finalised later this year and there have been informal suggestions of a transition period, but this is unconfirmed.

In terms of progress, in September 2017 the European Council published the first revisions to the draft legislation which were followed up in October 2017 by the European Parliament's Report containing a draft resolution on the e-Privacy Regulation. In early December 2017 the European Council released a consolidated version of the e-Privacy Regulation which provides both a summary of the progress so far and can act as a basis for future work.

Direct Marketing

Opt-in consent

As discussed above, the e-Privacy Regulation has now been delayed. However, this does not prevent the move to an "opt-in" consent regime.

As noted in the A29WP consent guidance, opt-in consent for marketing will apply from 25 May 2018 due to the GDPR taking effect. To explain, this is not because the GDPR requires consent to be obtained for marketing as in most cases we would expect the legitimate interests ground to be relied upon under the GDPR. It is because of the way that the different pieces of legislation cross refer to each other.

Currently in the UK the e-marketing regime is governed by the Privacy and Electronic Communications Regulations ("PECR"). These do not define consent but apply the definition from the e-Privacy Directive. This is the Directive that PECR implements in the UK, and which will be replaced in future by the e-Privacy Regulation.

The e-Privacy Directive currently cross refers to the definition of consent in the Data Protection Directive which of course will be repealed and replaced by the GDPR. The GDPR specifies that references to the Data Protection Directive will from 25 May 2018 be interpreted as references to the GDPR. Thus the reference in the e-Privacy Directive to the definition of consent will, from 25 May 2018, be interpreted as a reference to consent as defined under the GDPR.

As valid consent under the GDPR requires there to be clear affirmative action, opt-in consent for direct marketing will therefore apply from 25 May 2018 regardless of the status of the e-Privacy Regulation.

Marketing to business contacts

Under PECR business contact details are dealt with differently to personal contact details. However, the draft e-Privacy Regulation suggests that there may be no difference in approach between personal and business email addresses. This would mean that the opt-out consent approach would not be allowed to continue in respect of business contacts either. If this is the case, when the final e-Privacy Regulation is published, consent of the "end-user" (i.e. the individual) would be required in both circumstances.

The Direct Marketing Association is lobbying to retain the current position but the outcome of this is as yet unknown. For B2B marketing it is therefore a matter of watching this space.

International Transfers

The EU-US Privacy Shield

The European Commission published its first annual report on the Privacy Shield on 18 October 2017, concluding that it was working well, providing adequate protection for personal data transferred to participating companies in the US. The report also proposed recommendations for improvement, including closer monitoring of US companies' compliance with their obligations, raising awareness about how EU individuals can exercise their rights and by boosting cooperation between privacy enforcers.

Subsequently, on 28 November 2017, the A29WP published its review of the Privacy Shield which was not as positive. Whilst it welcomed the efforts of US authorities to support the framework, it highlighted issues it had previously raised including the surveillance powers of US government authorities.

The A29WP demanded an action plan to address its concerns, prioritising the appointment of an independent US Ombudsman and new members of the Privacy and Civil Liberties Oversight Board. EU Data Protection Authorities have stated that if these issues have not been resolved before the introduction of the GDPR, they will ask their national courts to make a reference to the European Court of Justice ("CJEU") on the validity of the Privacy Shield.

European Commission review of adequacy decisions

The recent scrutiny on international transfers has led the European Commission to review the 12 adequacy decisions it has made regarding third countries. Foreign governments have been asked for written clarification regarding their privacy safeguards and have been visited by data experts. Bruno Gencarelli, Head of the European Commission Data Protection Unit, said "we are looking at them with the objective of keeping them."

A29 Adequacy document

On 28 November 2017, the A29WP published an updated Adequacy referential document, a working document updating previous guidance on transfers of personal data to third countries. Among other things, this sets out the core data protection principles required to ensure that the level of data protection in third countries is essentially equivalent to the one under EU legislation and the essential guarantees in respect of law enforcement and national security access to limit the interferences to fundamental rights.

EU standard contractual clauses ("model clauses")

The future of model clauses is uncertain following the Irish High Court's reference to the CJEU on 3 October 2017.

The background is that Maximillian Schrems challenged Facebook Ireland's use of model clauses for the transfer of data to its US headquarters amid concerns that such clauses do not provide adequate protection to EU individuals. The Irish High Court requested a preliminary ruling from the CJEU on the validity of the model clauses.[1]

If the CJEU rules that their use does not accord with the GDPR this would have far reaching effects given the wide spread use of model clauses. The CJEU's ruling on this matter is expected in late 2018 at the earliest.

Brexit

In November 2017 we wrote an **article** on the impact of Brexit on data protection and privacy. It considers the future partnership paper published by the UK Government as well as the position paper published by the European Commission. It then looks at the impact of Brexit on data flows to and from the UK and the implications for other aspects of the GDPR.

Data Breach

A29WP: data breach notification

This guidance is intended to provide clarity on the boundaries and expectations of handling a data breach notification under the GDPR. See our **article** that we published on this guidance.

Preparation is key

One of the sessions at our Data Protection and Privacy Forum discussed the broader implications of a data breach. Whilst there has been much focus understandably in data privacy circles about the mandatory notification requirements, it is important not to lose sight of other important workstreams. This includes communications, whether that be media, investors, employees or customers.

Morrisons court ruling

On 1 December 2017, the High Court ruled in the case of Various Claimants v Wm Morrisons Supermarket Plc. The lawsuit was brought by 5,500 current and former Morrisons workers seeking compensation over a 2014 data security breach in which payroll information of almost 100,000 staff was posted on the internet.

Langstaff J handed down a judgment that Morrisons was vicariously liable for the acts of its rogue employee, notwithstanding the earlier finding that the employee's acts were unauthorised and contrary to Morrisons policies.

[1] Data Protection Commissioner v Facebook and Maximillian Schrems

This demonstrates how the actions of one rogue employee can create potentially huge financial liabilities for a company, regardless of the fact that the company has sufficient policies in place and is not directly liable. Companies should therefore reassess the risk surrounding their processing activities, limiting employees access to data to only that which is essential to their role, and ensure they have effective response plans in place in the event of a breach.

Morrisons were given leave to appeal the decision and it has indicated its intention to do so (so watch this space).

Views from… Hong Kong

The impact of the GDPR in Hong Kong: change is in the air

The GDPR marks a significant expansion of the territorial scope of the EU data protection regime, and the EU's status as one of Hong Kong's largest trading partners means that the impact of the GDPR will be closely felt here.

Hong Kong already has a strong and sophisticated data privacy regime. Nevertheless, Stephen Wong, Hong Kong's Privacy Commissioner, observed that given the introduction of the GDPR and the fact Hong Kong's privacy regime is founded on the existing EU regime, it is time to undertake a thorough review of the territory's data privacy law.

A recent comparative study by the Privacy Commissioner's office identified nine major differences between the GDPR and the Hong Kong regime including mandatory breach notification, data processor obligations, new or enhanced rights of data subjects and the severity of sanctions.

The study noted that large administrative fines are permitted under the GDPR, whereas the Hong Kong regime currently does not permit the Privacy Commissioner to impose administrative fines or penalties (although he may serve enforcement notices on data users). The Commissioner's view is that allowing his office to impose administrative fines would deter non-compliance and bring the Hong Kong regime not just into line with the GDPR, but also other regimes such as that in Singapore. It has been suggested that any such regime for fines would need to have strict criteria, prescribe a fine limit and provide for an appeals regime.

This review may result in changes to the Hong Kong regime, although the pace of such change is unlikely to be quick, or indeed embraced in relation to some differences. Nevertheless, the Commissioner has said that the way forward for Hong Kong in light of the GDPR and the study should be to publish more guidance, ensure greater training for data users, encourage information exchange and sharing on issues and challenges relating to compliance with the GDPR and strengthen international cooperation between the Commissioner's office and overseas equivalents.

For further information on data protection and privacy issues in Hong Kong or Asia, please contact Kevin Warburton, a Senior Associate in our Hong Kong office and part of the Firm's global Data Protection and Privacy Practice.

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 have a call / meeting on a no charge basis to discuss your preparations to date and whether there are areas we can assist you.

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, employment issues, litigation, outsourcing or global corporate and regulatory investigations. All our fee-earners are therefore trained to spot and advise on data protection and privacy issues in their practice area with the assistance of our network of data protection and privacy advisers across the firm, including our overseas offices.

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 Data Protection and Privacy hub provides the extra level of expertise and experience required. The Data Privacy hub consists of partners and associates with expert knowledge of the law and market practice in data privacy. Our Data Protection and Privacy practice is co-headed by **Rebecca Cousin** and **Rob Sumroy** and includes in our London office partners **Richard Jeens**, **Richard de Carle** and **Duncan Blaikie**.

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