BRISTOWS

TOP 10

DATA PROTECTION 2017/18

in association with

PRIVACY LAWS & BUSINESS
DATA PROTECTION WORLDWIDE

www.privacylaws.com

#fearofthefine

#privacy

2

#everyonelovesthegdpr

6

7

#countdowntomay

8

#myths

9

 # timerunningout

#notbrexitagain

3

#bitmoji

#furbyiswatchingyou

5

1

The Data Protection Top 10 2017/18

For most of 2017, it felt like the clock was against us. Certainly, word had got out that there was a new law (GDP something?) and everyone wanted to do something about it. For a team of data protection lawyers, working on a topic that may in the past have been considered a bit niche/difficult/nerdy/dull/unimportant (please delete, as applicable), it was pleasing to see so many companies taking it seriously, some for the first time, and not only large household names and big tech companies one might expect but also smaller outfits where DP could hardly be said to be core to their businesses. It's been a busy year for everyone.

We hope that you enjoy this year's list, the order of which has, as in previous years, been produced using an entirely non-scientific approach of haggling, discussion and arm-wrestling. It is, as ever, just a bit of fun but hopefully also informative.

#data

#topten

#sexrobots

4

10

DATA PROTECTION 2017/18

TOP 10

10

Smart Toys

In today's technology-driven world, the pressure on parents to delight children with the latest electronic toys and gadgets on Christmas Day may be greater than ever before. If, unfortunately, that stack of pricey gifts failed to hit the spot this festive season, then maybe it's time to invest in a smart toy – a completely safe and not remotely creepy option to put that smile back on little Johnny's face, right?

2017 saw significant growth in the number of smart and connected toys coming to market, and this growth is expected to continue exponentially for the foreseeable future. These toys, often in the form of a robot, doll or soft animal, have the ability to collect vast amounts of personal data and, in many cases, will connect to smart devices via the internet. Functionality can range from voice command and recording to video and messaging, and even incorporate facial recognition.

It's easy to see the potential for parents to use these toys to 'spy' on their children, using the linked device to listen in to recordings made during play or review messages sent to friends. But if you think that's concerning, then consider the risks from outside the playroom. Research has shown that many of these toys use insecure Bluetooth connections, leaving the doors wide open for hackers to listen to, watch and even communicate with child users – one study showed a connected robot could be hacked to start spouting obscenities, for instance. That jigsaw puzzle you bought precious Molly-May this Christmas not looking so bad now?

So what does the GDPR have to say about all this? Is there any hope of safeguarding the privacy rights of our future generations?

First-off, the GDPR contains many more specific provisions designed to protect personal data relating to children. A connected toy that enables a semi-sophisticated hacker to listen to your child is not going to make the grade. Further, children under 16 require a parent's or guardian's consent before their data may be processed online (though note the lower threshold of 13 in the proposed UK Bill). So much of the onus is on parents to check out what their child may be exposed to before letting them loose on a smart toy. Of course, this relies on parents having a certain level of technical awareness, not to mention the providers of these toys actually meeting their 'notice' requirements under the GDPR by fully explaining how personal data is handled.

The GDPR's bag of tricks also includes requirements around Privacy by Design, carrying out data protection impact assessments and enhanced security provisions, meaning that privacy and security should be addressed from the development stage of new technologies. Yet it would seem that the developers of these connected toys currently favour 'cool' functionality over data protection.

So what does the future hold? As toys get smarter and more connected, should parents be urged to steer clear? Will it take a series of major child data breaches before developers and parents alike take note? Perhaps the ICO will use its enhanced powers under the GDPR to target unscrupulous non-compliers? Perhaps that Furby Connect Father Christmas so kindly left under the tree last month will be getting re-connected with his mates down at Argos.

9 Sex Robots

Yes, a flagrant act of clickbait, but also a recognition that sex, for better or worse, has been one of the most important drivers in technological development in the last 20 years. And in 2017, discussions about sex robots and connected sex toys have gone mainstream.

The influence of pornography on the evolution of the internet can't be overstated, and we're now seeing it have the same driving force in virtual reality (VR) and the Internet of Things (IoT). Of course there are innumerable legal and ethical questions posed by the automation of sex, but one of the most significant has to be what it means for our privacy – in what most people regard as the most 'private' sphere of our lives.

The more we move online to explore our sexual appetites, the more information about our sex lives we share with the companies who provide our internet connection, search engine, dating app, or online adult content. Part of this move online is, perhaps ironically, influenced by a desire for more privacy – people are more comfortable consuming sex if they don't have to buy it publicly, even though in fact we leave a far greater trace when we buy something or interact with someone online than if we just walk, anonymous, into a shop.

Up until recently, the link between sex and technology has been limited to online porn and e-commerce. But then came the IoT, and no one is interested in anything anymore unless it comes with an app and is connected to our smartphone – including, it would appear, sex.

Okay, it's still only a small minority of people who want a life-sized sex robot, but the IoT has had a huge impact on more mainstream sex toys. These devices increasingly come with the ability for you, your partner (or even strangers in a chatroom) to control them remotely via the internet, for them to remember your preferences and even use machine learning to personalise your experience – all of which means a record of your sexual activity is likely being collected and stored in the cloud. The impact of this was first recognised by those looking at the (seemingly innocent) data collected by fitness bands, who noticed lots of users 'exercising' at odd times of night. Never before has our sexual activity been available in such granular detail for those with access to the data to mine and analyse.

Personal data about a person's sex life is (and will continue to be) 'special category data'. The starting position, therefore, is that providers will need to get explicit consent to process this data in an identifiable form, but there is no doubt that the data at an anonymous level is still valuable from a research and product development perspective. However, the risks don't necessarily all stem from the tech provider. What of the hackers, blackmailers and ex-partners? Ultimately, unless everything is stored locally on the device, it is difficult to protect your data entirely from intruders.

A final thought on VR, which in a few years could allow individual users to create their own virtual world. It seems inevitable that one of the first things people will want to create virtually is sex and, in all likelihood, not only with fictional characters. What happens when someone can create virtual porn featuring an ex-partner? The law may need to be extended to address this, considering the 'household exemption' in data protection law and the limited protection granted to image rights in the UK.

8 One-Stop-Shop

The One-Stop-Shop is generally viewed by the international business community as one of the most positive aspects of the GDPR. Organisations operating across the EU can avoid the nightmare scenario of having to deal with 28 (or 27?) different data protection authorities (DPAs) and facing potentially multiple fines (28 x 4% anyone…?). Instead, they will only need to work with one – their lead authority, 'sole interlocutor', or One-Stop-Shop (OSS).

The OSS will be the DPA in the country where the organisation has its 'main establishment' – the place of its central administration in the EU. In 2017, the Article 29 Working Party published guidance for organisations on how this would be assessed, and when it would apply. Significantly – by focusing on where the decisions about the purposes and means are made – the guidance effectively conflates the concept of the controller with the main establishment. This suggests that, to appoint an OSS, a multi-national must find an entity in the EU where decisions are made about the purposes and means of processing, i.e. an EU controller.

And this appears to be the direction of travel. It has always been the case that the OSS would not be available to organisations without an establishment in the EU. However, rumours abound that the DPAs' position is that the OSS is also not available to controllers outside the EU who are 'established' in the EU by means of a branch or subsidiary. Rather, the controller itself must be in the EU – despite the conflicting suggestion in the WP29 guidance that a non-EU controller can 'designate' a main establishment.

This position creates a number of challenges for multinationals headquartered outside the EU, who now have to convince the DPAs that an EU entity exercises sufficient 'control' to be an EU controller in its own right, and therefore can benefit from the OSS. Companies headquartered in the UK are similarly concerned, hoping that having decisions made in the UK will not count them out of the OSS.

All this has led to a number of multinationals seeking to bolster their EU27 presence as regards data protection and appointing DPOs and privacy staff – particularly in Ireland. In light of Brexit, Ireland has become the favoured destination for US companies looking for an English-speaking regulator who is (at least perceived to be) pragmatic and relatively business-friendly. There has never been a better time to be a DP expert in Dublin...

What the guidance didn't shed any light on is how the OSS will work in practice, and it's clear there are many challenges ahead. Partly it will depend on the ability of the lead DPA and other concerned DPAs to work together; however, the existence of divergent national laws and the prospect of appeals in the national courts mean that questions of jurisdiction will always be able to be resolved informally by the DPAs.

7 Schrems

In a year of prequels, sequels and never-ending franchise movies, it was nice to see the world of data protection getting in on the action with the announcement of Schrems II: This time it's personal (data).

We all remember the widespread panic that followed the blockbuster decision in Schrems I to invalidate Safe Harbor. While the potential implications of the decision were huge, the fears that Europeans wouldn't be able to access Amazon, Facebook, Google or Microsoft services were grossly overstated. US companies had other ways of getting their data to the EU and so things carried on as before. And the lasting significance of Schrems I isn't the invalidation of Safe Harbor (we've moved on to bigger and better things with Privacy Shield), but lies in the CJEU's willingness to vindicate the privacy rights of individuals in the face of enormous political pressure.

Now, following the Irish High Court's 'well-founded concerns', the CJEU is being asked to rule on the validity of the Standard Contractual Clauses, the most commonly used transfer mechanism. A decision finding these to be invalid would leave global organisations with very few realistic options to carry out global transfers of data with Privacy Shield surviving on political goodwill alone. Judging by Schrems I however, these challenges and inconveniences for business are unlikely to influence the CJEU. But we do believe that there are some important distinctions between Schrems I and Schrems II, and so we're not ready to write off the Standard Contractual Clauses just yet.

Whatever the fate of the Standard Contractual Clauses, it's hard to criticise those concerned with US surveillance practices. While the US had taken steps post-Snowden to address concerns, continuing this doesn't seem to be at the top of the Trump administration's agenda. The role of the Ombudsman created to deal with privacy queries from those in the EU and cornerstone of Privacy Shield has still not been filled. Such indifference makes the EU Commission's job of standing over Privacy Shield and Standard Contractual Clauses even harder politically.

One of the more difficult aspects for the US to accept is the perceived hypocrisy of those in the EU. Many of these countries also adopt questionable surveillance practices, including the UK. Conveniently though, these countries benefit from a legal exemption which means that their practices do not need to meet the exacting standards expected of those outside the EU. For those in the US it may seem like the game is rigged.

For now at least, things will carry on as before. Schrems II is still some way off and in the meantime, we are expecting the EU Commission to exercise its significant political influence to keep the show on the road by creating new and improved Standard Contractual Clauses or even Privacy Shield 2.0. Unfortunately for those of us in the UK, however, the EU Commission's pragmatism and support for global data flows and trade won't be on show during the Brexit negotiations. As we'll be discussing later on, the UK desperately needs mutual recognition of its privacy laws with the EU post-March 2019. Given the progress of the negotiations so far and the current state of the UK's surveillance laws, it's is not easy to be optimistic…

A year in numbers...

67% of fines levied by the ICO in 2017 were issued to private entities.

54

the number of monetary penalties issued by the ICO in 2017, for breaches of the DPA and PECR

2593

the number of US companies registered with Privacy Shield as of January 2018.

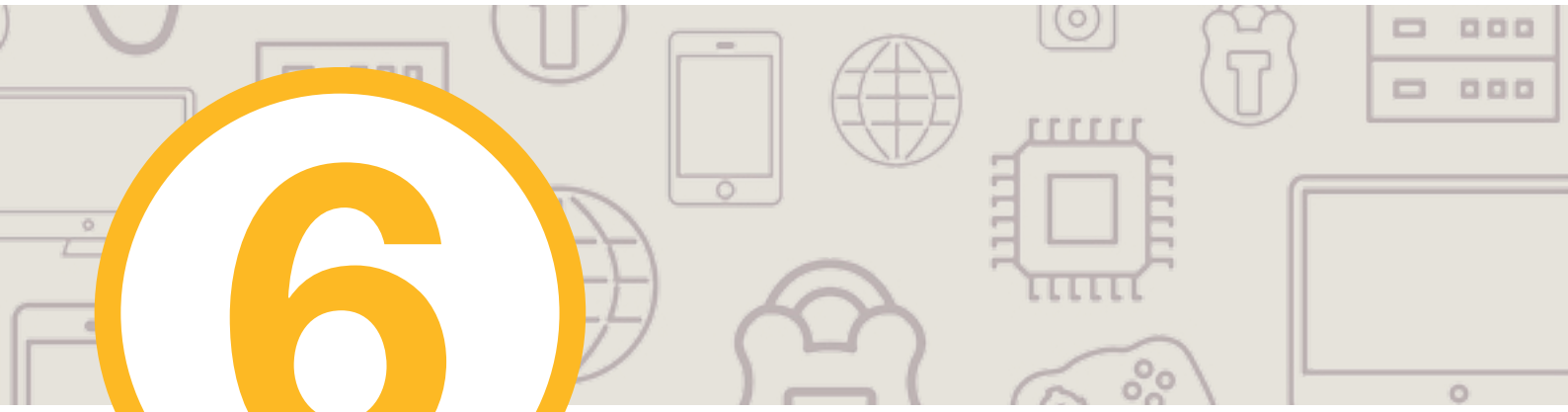
13 fines levied by the ICO were for at least £100,000

£78,472 was the average fine issued by the ICO in 2017.

20% of fines levied by the ICO in 2017 were issued to charities.

£400,000 was the highest fine levied by the ICO in 2017.

20 more fines were issued by the ICO in 2017 than in 2016.



6 Enforcement

With the spectre of the GDPR's increased fines looming large, regulatory action and fines levied in 2017 were scrutinised more closely than ever for an indication of how data protection authorities may flex their muscles come 25 May 2018. Record fines in certain European countries have made this an interesting (if potentially worrying) year indeed.

In 2017 the Information Commissioner's Office (ICO) also welcomed a new Information Commissioner, Elizabeth Denham. Last year we speculated whether (and how) her appointment and a new pair of hands at the helm would change the course of the ICO's enforcement activity…

Well, the ICO has had a busy year, and yet again the trajectory of enforcement action is on the up. A total of 54 monetary penalties were issued (up from 34 in 2016). Thirteen of the fines issued by the ICO were for at least £100,000 and the ICO matched its record-breaking fine of £400,000 (set the previous year against TalkTalk), issued this year against Keurboom Communications Ltd for making a staggering 99.5 million nuisance calls. Caboom indeed…

The ongoing investigation into the fundraising practices in the charitable sector led to 13 charities facing enforcement action in 2017 (and the tail end of 2016), totalling £181,000. The fines were levied for breaches of the First and Second Principles of the Data Protection Act (DPA) – fairness and purpose limitation – in particular for a practice known as wealth screening and sharing the personal details of donors.

As in the previous few years, most of the ICO's fines related to breaches of the Privacy and Electronic Communications Regulations but the percentage of fines for breaches of the DPA were on the up (and this time not just for breaches of the Seventh Principle relating to data security). Bolstered primarily by the action taken against certain charities, 22% of the fines related to breaches of the First and Second Principles of the DPA serving as an important reminder that enforcement action can follow a serious breach of any of the Principles, not just those relating to data security.

With the new Information Commissioner came a tendency for the ICO to issue public statements on high profile ongoing investigations. This new tactic, evocative of the 'naming and shaming' practices more readily deployed by the US Federal Trade Commission (FTC), is a development which will increase the public profile and scrutiny of investigations into an organisation's privacy practices, not just the enforcement action (if any) taken against them.

The Italian data protection authority (the Garante) sent shock waves this year when it set a European-wide record and fined a company €5,880,000 for breaching rules relating to consent. The fine was compounded by the company's (significant) dodgy dealing and money laundering practices, but does show a willingness from a European authority to take enforcement action which is more reflective of the fining powers provided under the GDPR.

How data protection authorities will deploy their new enforcement powers will unfortunately not be clear until we are faced with a breach under the new legislation. For now we have the guidance issued by the Article 29 Working Party, which stressed emphatically that authorities must be consistent in their approach (both in terms of fines imposed and the enforcement method deployed), and indicated that a breach may be considered intentional where it is the result of an organisation going against the advice of its data protection officer. It also made clear that a parent company will be on the hook for its subsidiaries, clarifying earlier confusion. But as always with enforcement, the proof is in the proverbial pudding, and we await next year's statistics with a higher than usual level of anticipation.

5

GDPR Myths

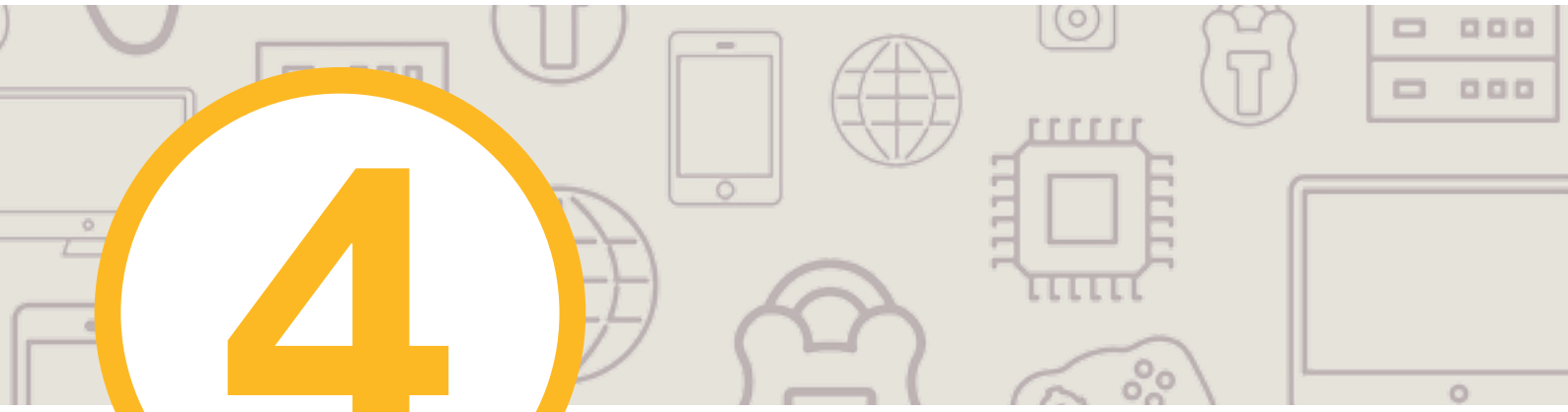
You may have heard quite a few myths over the year that have exaggerated the impact of the GDPR. Scary headlines generated the desired publicity, but some were due to genuine misconceptions about the new law which are important to de-mystify.

One myth involves consent, with many thinking that consent is always required. However, consent is only one of a number of legal grounds for data processing. It is true that rules around consent are being tightened, and this may cause headaches if consent is the only ground relied upon. As a result, privacy practitioners have been emphasising that it may be better to consider alternatives, such as performance of a contract in relation to employee data, or legitimate interest in relation to CCTV. These grounds will not leave a controller hanging if consent is withdrawn, and may help them to continue the data processing unless, of course, the individual has validly invoked their right to object to it. What's more, the legitimate interest ground has received positive clarification under the GDPR, and new grounds have been created for the processing of special categories of data, such as in relation to pharmacovigilance – both making it easier for controllers to find other, appropriate alternatives to consent. In addition, the assertion that public authorities will not be able to rely on legitimate interest may not always be true – it has been proposed that UK public authorities will be able to do so, addressing the need of universities, schools and colleges to process alumni data for fundraising purposes and other data for ancillary activities.

A second myth is that individuals have an absolute right to erasure; in practice, there will often be a good reason to retain at least some of the data about an individual. For example, where the processing is based on consent to receive marketing communications which has been withdrawn, the controller will have to comply with a request for erasure of data which was processed on the basis of that consent. However, this does not mean that the controller may not retain data about past sales that must be kept under tax rules, or a record about the request on the customer services system. So the scope of the right will vary depending on the circumstances and counter-intuitively, individuals will often have to be remembered in order to be effectively forgotten.

Another myth is that everyone will be fined for minor non-compliance. As we've discussed, the power of regulators to impose fines of up to the higher of €20m or 4% of total annual turnover is a powerful tool. However, the ICO has downplayed the extent to which the highest penalties will actually be dished out. Only a small proportion of regulatory investigations result in fines, and the maximum fine has never been invoked. The purpose of fines is not to fund the regulators, and those organisations that are genuinely moving in the right direction without unreasonable delay are unlikely to be penalised excessively for minor breaches. In addition, fines that are not 'effective, proportionate and dissuasive' may be challenged in courts, some countries are introducing a pre-award judicial review before a fine is imposed, and under the GDPR, a post-award judicial review must be available in all jurisdictions.

Finally, contrary to the warnings that Europe is short of 28,000 DPOs, most private organisations may not even have to appoint a DPO. For the private sector, the requirement is triggered only where the organisation's core activities consist of, or are inextricably linked with, processing operations that require regular and systematic monitoring of data subjects on a large scale or of processing 'sensitive personal data'. These might include: those concerned with the processing of images, such as CCTV security services; personal advisors, such as immigration consultants and lawyers; and potentially marketing and advertising agencies, provided that other criteria are satisfied. However, processing related to workforce administration or the usual in-house marketing activities, including profiling, are not likely to trigger the requirement.



4 Brexit

Appearing inevitably in our leader board like that boring relative at the party that nobody wants to invite, Brexit is, unfortunately, this year's number 4. Despite everyone's best efforts to ignore it, Brexit is still on the cards and, we are assured, due to happen at exactly 11pm on Friday 29 March 2019. And as well as usurping the weather as Britain's favourite conversation filler, Brexit is throwing up some pretty significant data protection issues, mostly related to how on earth we'll navigate data transfers in this brave new post-EU world.

- Brexit and the EU

We move so much data between the UK and the EU that it's crucially important to get these transfers as seamless as possible after Brexit. Most agree that the best solution would be an adequacy decision from the European Commission, which would mean that the UK's standard of data protection would be considered 'essentially equivalent' to the EU's, minimising restrictions on cross-border data sharing. So far so good, and with the new Data Protection Bill implementing much of the GDPR word for word, the British Government seem pretty confident that adequacy can be achieved. However, as many (including the House of Lords) have pointed out, this decision is not just based on data protection legislation, and certain areas of the UK's national legislative framework (especially regarding privacy and surveillance) may be just too divergent and therefore preclude an adequacy finding.

There's also an issue with timing, as we'll only be able to start the adequacy procedure once we leave the EU. What exactly will happen with UK-EU transfers whilst we're waiting for the adequacy decision to be made?

And even if we do get adequacy, it's not then a case of patting ourselves on the back and considering it a job well done. Our position as an adequate 'third country' will be under continual scrutiny, and may well require renegotiation time and time again. With the Commission able to withdraw their decision as they see fit, it's entirely possible that future changes to our data protection legislation or, more likely, the introduction of additional surveillance powers, may cause us to lose our adequacy status and put us back to square one. So unfortunately it's clear that adequacy isn't the miracle cure we'd like it to be, and we're likely to be facing uncertainty with EU-UK transfers even after Brexit has happened.

- Brexit and the US

A second key issue is how to regulate transfers between the UK and US after Brexit. It's unlikely that Britain will be able to rely on the current Privacy Shield framework unless we remain part of the EEA, but will a UK-US equivalent (like the parallel Safe Harbor arrangement between the US and Switzerland) be a suitable and feasible alternative? Will the British Government wish to negotiate a completely different agreement? And what will happen with onwards transfers from the UK under the EU-US Privacy Shield? At the moment, there seem to be more questions than answers on the topic, and with numerous EU institutions still questioning the sufficiency of certain aspects of the existing Privacy Shield, it's not easy to say when we'll get the clarity we're waiting for.

So in a characteristically Brexit fashion, we still just don't know what international data transfers will look like once Britain has left the EU. And as this uncertainty is so damaging for businesses both here and overseas, we need to remain hopeful that our government will start making those crucial arrangements and decisions soon, whilst we continue to do all that we can contractually to minimise the disruption that Brexit is likely to cause.

3 Data Protection Bill

2017 saw the publication of the UK Data Protection Bill, promptly silencing those who thought that Brexit would spell the end for the GDPR in the UK.

At an eye-watering 218 pages long, thankfully only a small proportion of the Bill is actually relevant for most companies, and most of us can merrily skip past provisions covering the processing of personal data by the intelligence services and the implementation of the Law Enforcement Directive.

As expected, the Bill is closely aligned with the GDPR, as this is essential to the Government's hopes to obtain an 'adequacy decision' (set out in their August 2017 publication 'The Exchange and Protection of Personal Data – a Future Partnership Paper'). Whilst there is nothing particularly novel or transformative about the Bill, several notable points of interest include:

- Children's data: the GDPR provides that domestic law can determine the age at which a child can consent to their data being processed by providers of information society services (i.e. online services) as long as this is between 13 and 16. As expected, the Bill confirms that in the UK, this will be 13.

- Conditions for processing special categories of data and criminal convictions data: data controllers processing special / criminal data in an employment context or on grounds of substantial public interest will need to implement an 'appropriate policy document' as an additional safeguard which explains how they comply with the Data Protection Principles and how long the personal data is likely to be retained for. The policy document must be reviewed and updated and made available to the Information Commissioner's Office (ICO) on request.

- Automated decision making (ADM): whereas historically ADM has been seen as a 'right' that data subjects need to exercise in the UK, rather than a 'prohibition', the Bill (and indeed the Article 29 Working Party) indicates that ADM is in fact an outright prohibition unless one of the narrow exceptions apply (i.e. necessary for the performance of a contract, authorised by Union or Member State law or explicit consent). This somewhat unexpected interpretation presents a massive practical challenge to several sectors (particularly financial services) who make thousands of automatic decisions on a daily basis and who may struggle to find an appropriate exception upon which they can rely.

- ICO funding: the ICO will be able to require data controllers to pay charges to its office and may also charge fees for providing certain services. This answers the question of how the ICO will be funded once notifications are abolished.

The Bill will likely enter the House of Commons for its first reading in early 2018.

2 The ePrivacy Regulation

In last year's Top 10 we reported on the draft ePrivacy Regulation – the official proposal for which had just been published by the European Commission in January 2017. A lot has been discussed regarding the ePrivacy Regulation over the course of the year, a lot has been debated, and a lot has been lobbied – however, not a lot has actually changed.

Since the Commission's official proposal was published, we've had opinions from the Article 29 Working Party and the European Data Protection Supervisor in April, and we've also had multiple opinions and reports from various European Parliament Committees over the course of the year (including the Committee on Industry, Research and Energy, the Committee on the Internal Market and Consumer Protection, and the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee).

After a batch of opinions and reports were published halfway through the year, we then received the draft counter-proposal from the Council of the EU published in September. Not wanting to be left out, the LIBE Committee then published its draft in October. All the while, the online advertising industry has been lobbying furiously over what it perceives to be an overly conservative piece of regulation which doesn't reflect the realities of how the industry actually works.

While the outcome of the ePrivacy Regulation is still uncertain, what is definitely clear from the various reports and opinions published over the course of 2017 is that there is a significant gap between the expectations of the various European institutions and those of industry.

What also became clear was that the aim of finalising the ePrivacy Regulation so that it could apply from May 2018 (nicely coinciding with the GDPR) was, to put it mildly, a tad unrealistic. The way the negotiations and lobbying have gone so far in Brussels, particularly if the GDPR was anything to go by, we'll be lucky if the ePrivacy Regulation comes into force before 2019 (or perhaps unlucky, depending on your viewpoint…).

Some of the most contentious and heavily lobbied elements have included: (i) the expansion of the consent requirements for e-marketing to include B2B marketing; (ii) the escalation of the cookie consent requirements so they operate at the 'browser' level; and (iii) the express prohibition of conditioning access to a digital service on providing consent for tracking cookies. Other big ticket items include the expansion of the scope of the framework to cover communications services provided over the internet (so-called 'over-the-top' or OTT services, such as Skype, Messenger and WhatsApp) which imposes greater obligations to secure the confidentiality of communications.

The outgoing Estonian presidency published a progress report in November in which it suggested, amongst other things, that the position regarding browsers and cookies was by no means settled and that further analysis and discussion were required in these areas. One of the key discussion points has been, in the words of the Commission, finding a 'balance between ensuring proper privacy protection without undermining legitimate business models'.

However, what has remained consistent throughout the various discussions is that: firstly, the ePrivacy Regulation is, as the name would suggest, a Regulation. Whatever happens, there will at least be more harmonisation than the currently fragmented regime under the ePrivacy Directive. Secondly, the potential fines will mirror the regime and larger amounts set out in the GDPR. Thirdly, whenever consent is required under the ePrivacy Regulation (whether for cookies or e-marketing), this will be 'GDPR-grade' consent with all the bells and whistles that comes with it – a significant challenge for the adtech industry

in particular. Finally, whether they like it or not, the OTT providers will be caught within the scope of the new regime – it's just not clear yet what being within scope will actually mean.

Once the trilogue negotiation gets into full swing, with any luck the mist should clear, and hopefully digital businesses and online advisers will get some desperately needed clarity about the extent to which the new regime will affect their business models. As we said at the end of last year, what is clear is that the Commission is not satisfied with the GDPR alone and intends to double down on the regulation of OTT providers and the online tracking industry. If the Commission gets its way, there will be some extremely tough challenges for the online industry ahead (as if the GDPR wasn't enough to worry about…).

1

Coming in at number one...

Accountability

There was once a time when for most companies, 'data protection compliance' meant little more than a line of small print at the end of a paper form, possibly with a tick-box, and asking the HR team to be discrete with the personnel information crossing their desks. As a result of the GDPR, the world looks very different now – at least for companies taking it seriously, which many are. In the last twelve months alone, the Bristows data protection team has helped over 50 companies, almost all multinationals, to implement the 'accountability' requirements of the GDPR, making 'accountability' worthy of the top place in our Data Protection Top 10.

What does 'accountability' look like? In most cases, a set of policies and controls, supported by trained staff, implemented throughout the business. These policies distil the GDPR down to manageable, user-friendly documents which address specific issues – handling HR data, direct marketing, contracting with suppliers, conducting privacy impact assessments, Privacy by Design, and so on. Documents that apply the GDPR to a company's business in context enable staff who handle personal data to follow simple internal 'rules' without having to worry about the detail of the GDPR itself.

Many of these policies and controls are similar from company to company. The requirements for Privacy by Design and handling HR data don't vary greatly, although their significance to a company may do, depending on its line of business and headcount. In other areas, there can be more varied processing issues that are particular to a company's sector – adtech, financial services regulatory, cloud computing, whatever it might be. It's important that any policies and controls are a good fit with the business, and we've found that the way to best understand a company's business and the processing issues involved is through conversation with the right people, whether via workshops or otherwise. We avoid detailed processing questionnaires like the plague. They seldom provide much useful information, and it's better to talk to people, with the added benefit of providing education and greater context for the project.

In many ways, developing the accountability documents is the easy part. They then need to be implemented across multiple

business units, subsidiaries and countries. This can result in a significant amount of 'change' internally – IT system changes, contract changes, process changes and the introduction of new compliance processes. Managing change across a large multinational can be both complex and time-consuming. Project management skills, whether internal or external, are essential. The following work streams are typical:

- Implementing the accountability documents. This is the process of bringing the various policies to life across the company. Many of the obligations set out will be met through the other work streams below. For example, a requirement that HR deletes CVs for unsuccessful candidates could be built into the recruitment system used and so picked up as part of the IT systems work stream, or it could be a manual 'HR process'.

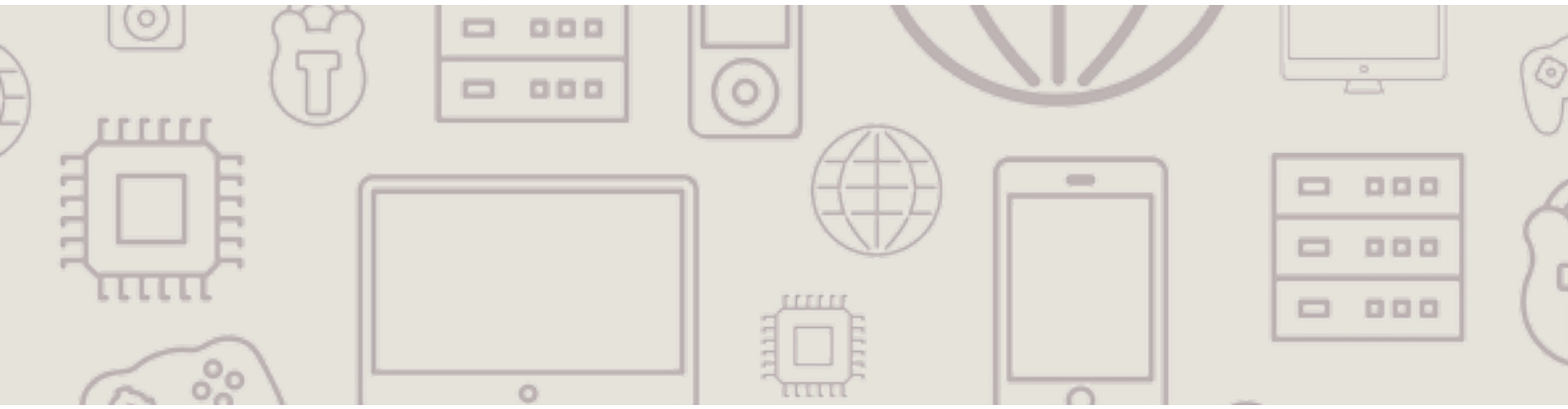
- Establishing an internal governance structure. Whether a company requires a formal Data Protection Officer under the GDPR or not, without an appropriate level of privacy resources internally, a GDPR program will fail. Under this work stream, a Privacy Office may be established, together with a network of trained 'privacy champions' – individuals with a good level of compliance knowledge across the various internal functions.

- Updating the company's 'touchpoints'. Wherever a company collects personal data, it's likely to need to provide a detailed notice to the individuals concerned, whether through an online policy, a call-centre script or a 'just in time' notice. This work stream involves identifying the various points at which personal data may enter or be created by a company, to make sure an appropriate notice is given and consent obtained (if consent is necessary) at each point.

- Updating contracts. Even a modest sized company will usually have lots of existing supplier relationships. For companies that are themselves service providers a lot of their customer contracts will also be subject to the GDPR. This work stream involves prioritising these contracts both in terms of privacy and business risk and agreeing a strategy to update them. Potentially, this is one of the most significant pieces of work.

- Updating IT systems. Some requirements of the GDPR may require changes to IT systems, such as enforcing a data retention policy, an IT security policy or looking at the various data fields processed to identify any that are excessive or unnecessary. This work stream involves identifying the priority IT systems (based on various criteria) and developing a plan for each one, to bring it into compliance.

Even for a well-organised project, prioritising the right issues and adopting a risk-based approach, there's a lot to do between now and 25th May 2018. But there's no need to panic. Of course, we tend to hear from the companies focusing on the GDPR as opposed to those that, for whatever reason, aren't. For a company yet to start, the time has come to take it seriously. It doesn't have to be a massive project with armies of consultants turning the company upside down. A modest,

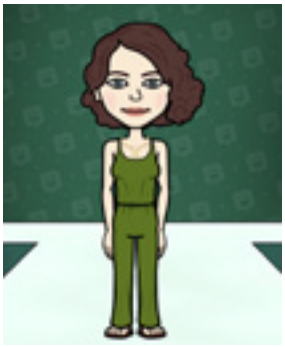


prioritised approach can be taken, focusing on the key issues, with a plan to get to everything else later on, after 25th May 2018 if necessary, perhaps long after. The most important thing is to start. We're not expecting a sea-change in enforcement culture amongst the EU DPAs – most sensible DPAs will be sympathetic to a company that is mid-flight in its GDPR program, with yet more to do. But with so much publicity about the GDPR over the last five years, there's likely to be less sympathy for companies that have made no attempt to comply. So, if you haven't already, it's time to start.

The **2017/18 Data Protection Top 10** was brought to you by...

Mark Watts
mark.watts@bristows.com

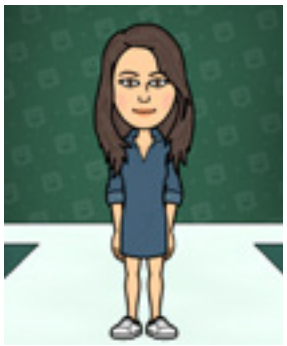
Sacha Wilson
sacha.wilson@bristows.com



Hannah Crowther
hannah.crowther@bristows.com

Alex Dittel
alex.dittel@bristows.com

Faye Harrison
faye.harrison@bristows.com



Rosalie Hayes
rosalie.hayes@bristows.com

Brian Johnston
brian.johnston@bristows.com

Emma Macalister Hall
emma.macalisterhall@bristows.com

Janine Regan
janine.regan@bristows.com

Katy Gibson
katy.gibson@bristows.com

Thanks for reading! Any questions, please get in touch.

International Report

Articles in recent issues included:

- Questioning 'adequacy'– Japan
- Australia's mandatory breach notification regime
- Blockchain: disrupting data protection?
- Poland takes further steps to adjust to the GDPR
- Austria amends DP law to comply with GDPR provisions
- Belgian DPA publishes guidance on DPOs and records
- Russia increases DPA's powers and fines
- Ireland's DP Commissioner optimistic on One-Stop-Shop
- Get contracts with vendors and customers GDPR ready
- EDPS: New e-Privacy law will mean stronger enforcement
- Germany's new DP Act: Big news or business as usual?
- Data protection – or protectionism by the back door?
- What is fairness in an algorithmic world?
- Heart on your sleeve: DP implications of wearable tech
- Hong Kong's DPA prefers mediation to prosecution

United Kingdom Report

Articles in recent issues included:

- Data Protection Bill debated at the House of Lords
- GDPR narrows opportunities to rely on legitimate interests ground
- The ICO retains its international horizon
- DPAs should fine only seriously negligent conduct
- The future of data protection law and enforcement in light of Brexit
- Woodland Trust turns over new leaf in collecting consent
- A Data Protection guide to the use of marketing data
- Machine learning: The future is in our hands – or is it?
- Beware of over caution implementing Privacy by Design
- UK marketers want more guidance on GDPR compliance
- Challenges to the EU-US Privacy Shield and the Model Contract Clauses
- GDPR: Data processing at work
- RNLI to sink or float with opt-in policy

PL&B Report Subscription Package

A subscription provides you with the following benefits:

12 Issues Per Year
You will receive six International Reports and/or six United Kingdom Reports per year.

PDF Versions
You will receive the PDF version of the latest issue on the day of publication and you will gain access to the latest issue from our website.

Online Back Issues
Access International Report back issues (from 1987) and/or UK Report back issues (from 2000).

E-Mail News Updates
E-mail news updates help to keep you regularly informed of the latest developments in data protection and privacy issues with the following options: worldwide; the UK; and the UK Freedom of Information Act.

E-Mail News Archive
Access to an online archive of e-mail news updates.

Online Search Tool
Search for the most relevant content from all *PL&B* publications and events. You can then click through from the search results into the PDF documents.

Events Documentation
Access International and/or UK events documentation such as our various Roundtables with Data Protection Commissioners and the *PL&B Annual International Conferences* in Cambridge, UK.

Helpline Enquiry Service
Contact the *PL&B* team with your questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. Please note this service does not offer legal advice or consultancy.

Special Reports
Gain access to *PL&B* special reports on data privacy laws worldwide, and a book published on Data Privacy Laws in the Asia-Pacific region.

Subscribe at privacylaws.com/subscribe

31ST YEAR

Privacy Laws & Business
31st Annual International Conference

Navigating to GDPR success: The art of the possible

2-4 July 2018, St John's College, Cambridge, UK

privacylaws.com/annualconference

Designed and Produced by ProCreative, Tel: 0800 228 9846

REPORT2PP 2.0 01/18

#privacy

2

#everyonelovesthegdpr

6

7

#countdowntomay

8

#myths

 # timerunningout

#notbrexitagain

3

5

#bitmoji

1

#furbyiswatchingyou

#fearofthefine

9

#data

#topten

#sexrobots

4

10

100 Victoria Embankment
London EC4Y 0DH
T +44(0)20 7400 8000

www.bristows.com
www.bristowscookiejar.com

This paper contains material sourced from responsibly managed and sustainable commercial forests, certified in accordance with the FSC (Forest Stewardship Council). It is produced using recyclable 100% ECF (elemental chlorine free) pulp; an environmentally friendly bleaching process.