BRISTOWS

TOP 10

DATA PROTECTION 2016/17

in association with

PRIVACY LAWS & BUSINESS
DATA PROTECTION WORLDWIDE

www.privacylaws.com


#snooping
#spam
#privacy
#geek
2
1
#artificalintelligence
6
#nofilter
7
#topten
#brexit
#cookies
10
#newentry
8
#privacyshield
#dataprotection
3

#nuisancecalls

5

#hashtag

#bristowscookiejar

The Data Protection Top 10 2016/17

2016 was, well, an "interesting" year. In between Brexit and Trump, there was plenty of news (and a few surprises) on the data front as well. Technology continues to develop at an exponential rate, the tension between national security and privacy continues, and there appears to be no stopping Max Schrems. And of course, we're now just over a year away from the GDPR. All of which meant we had plenty of material to choose from in compiling this year's Top 10 data protection issues for 2016/17.

We hope you enjoy our list — even if some of you vehemently disagree with our order of priorities (there was plenty of lively discussion amongst our team as well...).

As for 2017/18, we're already placing bets on what makes the list next year.

#countdown

#selfie

9

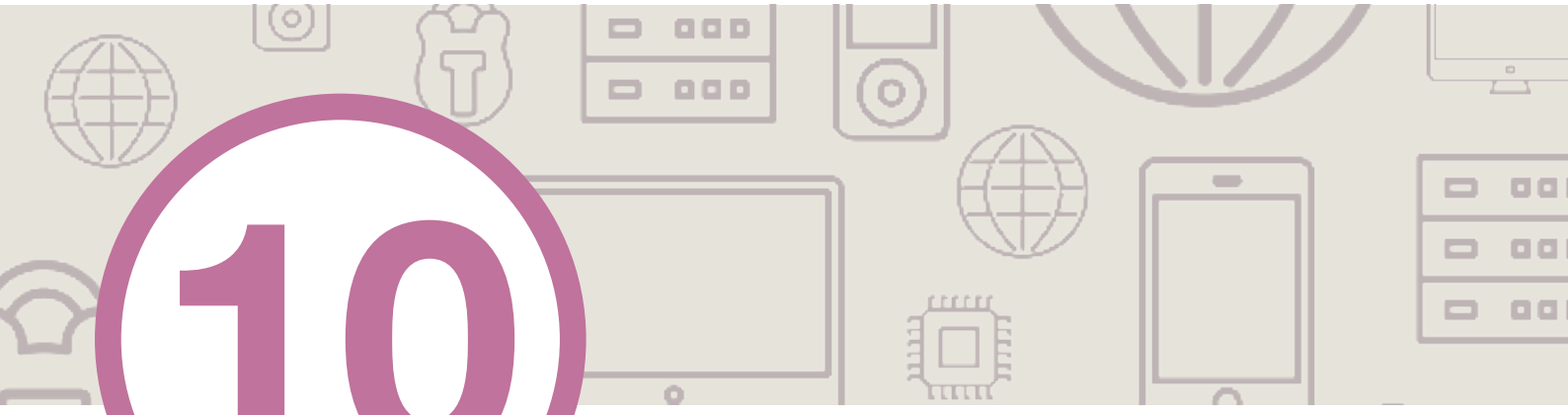
#data

#alternativefacts

4

DATA PROTECTION 2016/17

TOP 10



10

Compensation for breaches of the 1998 Act

Starting our list at (cynics argue) the heart of everything: money. Since the 2015 Court of Appeal's judgment in *Vidal-Hall v Google* opened the door to potential claims for 'mere distress' caused by a breach of the Data Protection Act 1998 (DPA), many have been speculating on the level of damages likely to be awarded for this new head of loss. 2016 brought with it some interesting case law in the form of (not so anonymous) Home Office statistics and a police officer's trip to Barbados. None of the awards reached anywhere near the levels of the phone hacking cases in 2015, but the amounts in both cases were still significantly more than a 'nominal' sum.

In *TLT and others v Secretary of State for the Home Department*, the Home Office published statistics on the UK Border Agency website using a spreadsheet which (unintentionally) contained the names of 1,598 family members, their age and nationality, whether they had claimed asylum and the office which dealt with their case.

The Court awarded damages to the individuals affected ranging from £2,500 to £12,500, including children of the 'lead applicant' whose identity could be inferred, even though they were not explicitly named. In making the award, the Court made a number of interesting points regarding awards for distress, including that 'sudden shock' is sufficient to constitute distress, and that distress awards should be commensurate with awards for less severe psychological injury. In considering the amount of an award, the Court will conduct a close examination of the claimant's individual experience, as well as the rationality of their fears.

In the County Court case of *Andrea Brown v The Commissioner of Police of the Metropolis*, Ms Brown, a former police officer, was awarded £9,000 in damages for distress for breach of the DPA and misuse of private information. An officer in her station had used police powers designed for investigating crime to obtain information about Ms Brown's holiday plans, after she travelled to Barbados without notifying her line manager — including applying to Virgin Atlantic and the National Border Targeting Centre. In doing so the police officer had cited a non-existent statute - the "Police Act 2007". The police admitted breaching the DPA and Ms Brown's right to privacy under Article 8.

In an out of court settlement, Manchester Police agreed to pay a victim of domestic violence £75,000 after her case history was used in a training exercise without being anonymised. The woman had agreed to the material being used on the basis that her identity would not be revealed, but it subsequently emerged that details including her identity, medical history and a 999 call recording were shown to various officers in training. The woman had brought a claim against the police force for misuse of private information, breach of confidentiality and breach of the Data Protection Act, which was ultimately settled out of court.

With the GDPR drawing ever closer, practitioners expect to see an increase in claims for distress (or, to use the GDPR wording, 'non-material damages') against both controllers and processors. The GDPR also creates the potential for an increase in 'class actions' of some sort, as (subject to local law) it allows not-for-profit bodies to bring representative action on behalf of individuals. Although the court awards last year were by no means massive, when multiplied by a class of 10s or 100s, they start to add up to some very significant numbers indeed.

9

Artifical Intelligence

In at No. 9 is artificial intelligence or "AI". Whether being used to improve medical diagnostics, be your personal assistant, or beating the world Go champion, AI-based solutions were popping up everywhere in 2016.

As with most of today's technologies, AI is data driven. It relies on algorithms to learn autonomously without being specifically programmed and can assist with profiling, prediction, decision-making, filtering or categorisation.

Precisely how AI systems fit with traditional data protection concepts needs to be given some serious thought. For instance, where it can make its own human-style decisions, could an AI machine qualify as a data controller or processor? If so, who would be held liable for any breach of data protection laws? Okay, so they don't sleep, dream or fall in love, but could an AI machine mimicking the human mind ever be regarded as a data subject?

Fundamental to any AI solution is the ability to constantly learn from its use. This, combined with the ability of AI to establish links within complex data sets, means that data that may not initially appear 'personal' can quickly become an extremely rich personal profile. A classic example of this is the driverless car. The car will collect information about how it is used to improve its own driving capabilities; this may not be collected for the purposes of profiling the human driver, but it inevitably results in a comprehensive profile of his or her driving and lifestyle — which could include their precise movements, how fast they drive and even how much they weigh.

One of the main challenges discussed in the AI community is how to provide individuals with an intelligible explanation of algorithmic decisions made about them, as required by the GDPR's transparency provisions. Without a PhD in incomprehensible tech-speak, how can users really understand the potential impact on them enough to make an informed decision?

Another question is to what extent the GDPR's grounds for conducting automated decisions can be satisfied in the context of AI. As it's not easy to predict in advance precisely how data will be processed by a self-learning algorithm, it may become difficult for data controllers to justify that consent is sufficiently 'informed' or that the AI is *necessary* to enter the contract.

Accuracy of the output generated by an AI system is a frequently expressed concern by AI doubters, particularly where it automatically results in decisions being made without any direct human involvement. AI proponents will argue that machines are significantly less prone to error than humans — and that this is the key value of AI. The GDPR will require controllers to offer the right to obtain human intervention of any automated decision and contest the decision. It is questionable how practicable this will be in many circumstances and whether it could ultimately undermine the entire value of the AI — if every decision has to be reviewed by a 'mere human'. As with other data dependent technologies, Privacy Impact Assessments, 'Privacy by Design' and 'Privacy by Default' will be essential tools for any AI developer to show that privacy issues have been carefully considered in respect of any AI-based solutions.

8

What is Personal Data?

The *Breyer* case, the new concept of "pseudonymous" data in the GDPR, and the unstoppable increase in the use of online identifiers meant that 2016 saw data protection gurus continuing to grapple with the ultimate existential question — when is data "personal"?

Of course, we all know the answer: data is personal when it relates to an identified or identifiable living individual. So far, so simple. And it's generally accepted that "identification" does not have to mean knowing someone's name and address. However, in an increasingly connected and personalised world, what does it mean to be identifiable? At what point does the IP address 192.168.1.97 become not just a number, but a vital piece of information about me, enabling a business to follow my activities online, track my location in real-time and find out who I'm interacting with?

It is increasingly posited that *identification* should, in fact, be treated as *individuation*. This means that provided you can tell that person A is distinct from person B, it does not matter that you don't know who person A or B are. Proponents of "individuation = identification" point to Recital 26 of the GDPR for support, which refers to "singling out" in explaining the concept of identification.

One can see why this idea is popular with some regulators in an online context. Businesses may never know the name of a user, but they can still build up a detailed profile of them based on their online activity — and use this to show them targeted content. But the logical conclusion to this is that anonymous data can only ever be *aggregate* data. Any data which relates to a single *person* must be personal data, with no need to consider whether that person is genuinely at risk of being identified. This presents some obvious headaches in the area of medical research and clinical trials, for example, as it prevents patient level data from ever being anonymous.

It has been said that claiming IP addresses aren't personal data is akin to still arguing the world is flat. The GDPR specifically refers to "online identifiers" in its definition of personal data (albeit only if they cause an individual to be "identifiable"). For some, therefore, the CJEU's October ruling in *Breyer* regarding dynamic IP addresses came as something of a surprise.

In *Breyer*, the CJEU was asked whether the fact that a third party (in this case an ISP) held additional data, which would enable the data subject to be identified from the IP address, meant that it constituted personal data in the hands of the website operator. The CJEU said "no:" a dynamic IP address will not be personal data simply because any third party possesses sufficient additional data to identify the individual; the website operator must *also* have the *legal means* of obtaining the additional data.

In a divergence from its recent more activist stance, the CJEU appeared to reaffirm its support for a genuine test of 'identifiability'. If the individual is not already identified, it must be reasonably likely that the data controller could combine the data with other data to work out *who* the individual is. The fact that someone else holds this key is not, in itself, sufficient.

As big data analytics tools increasingly allow data to be combined and analysed for trends and profiling, it seems unlikely that *Breyer* represents anything other than a brief reprieve under the existing Directive. Come May 2018, It's Personal.

7 Enforcement

Fines issued by the ICO have once again made the headlines this year. The record for the highest fine ever was broken not once, but twice. The ICO issued a fine of £350,000 in February for automated marketing calls, only to raise the bar again in October with a £400,000 against TalkTalk for their failure to manage a cyber-attack.

With just over a year until the GDPR becomes applicable, and with it the potential for eye watering fines of €20 million or 4% of global turnover, enforcement action taken by the ICO has never before been the subject of more scrutiny.

Spam text messaging and nuisance calls were the main source of fines for 2016, making up just under 70% of the total penalties and totalling a massive £2 million for the whole year. In February, a fine of £350,000 (at the time the largest ever recorded) was issued to Prodial Ltd, who were found to be responsible for more than 46 million automated nuisance calls.

A second record-breaking fine of £400,000 was issued in October against TalkTalk, for the telecoms group's failure (according to the ICO) to *'implement the most basic cyber security measures'*. Exploiting a well-known flaw in TalkTalk's systems, a 17 year-old hacker launched a cyberattack and accessed the personal data of 156,959 customers, including the bank account and sort code of 15,656 customers. It was not a good day for TalkTalk.

Reminding us that it's not all about cyber security, 2016 saw the ICO continue to issue penalties for failing to secure physical documents as well. Hampshire County Council was fined £100,000 after it left documents containing personal details of over 100 people in a building the Council had previously occupied. Two significant fines were also issued against public bodies whose staff made the classic error of failing to check email recipients before hitting the 'Send' button. A Welsh police force was ordered to pay £150,000 for sending an email identifying eight sex offenders to a member of the public, and a London NHS trust was fined £180,000 after revealing the email addresses of more than 700 users of an HIV service when it sent out its monthly newsletter.

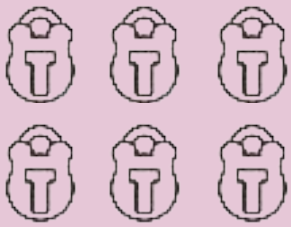
Although the Data Protection Act fines continued to be focused on primarily the seventh principle, they were not exclusively so. The ICO issued two fines against the British Heart Foundation and the RSPCA for breaches of the first and second principle, as part of a wider investigation into fundraising practices in the charitable sector. It serves as a reminder that fines can not only be issued for hacks and leaks, but also for any serious breach of the principles.

With a new Information Commissioner in place and the application of GDPR just around the corner, we expect the fines issued in 2017 to be watched *very* closely as a key indicator of how enforcement under the GDPR will be managed — and just how eager the ICO will be to show its newly sharpened teeth...

A year in numbers...

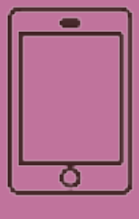
£400,000 the monetary penalty issued to Talk Talk in October, the largest fine by the ICO to a single data controller

35
The number of monetary penalties issued by the ICO in 2016, for breaches of the DPA and PECR



1,390
the number of US companies registered with Privacy Shield as at January 2017

12 months for which a telecommunications provider can be required to maintain communications data under the new Investigatory Powers Act



£75,000
the amount of compensation Manchester Police agreed to pay a woman whose private information was used in a training exercise, for breach of the DPA, breach of confidence and misuse of private information

£500
the lowest fine, to a historical society which had an unencrypted laptop stolen

478 the number of days, from 01 February 2017, until the GDPR becomes applicable across the EU

£3,246,000 the total amount of fines levied by the ICO for breaches of the DPA and PECR (up from £2,030,250 in 2015)

6 Regulatory Convergence

Next up, it's regulatory convergence. Large, online technology companies (the likes of Google and Facebook) with billions of users and amassing more personal data than it's possible to imagine, have caught the eyes of the Data Protection Authorities over the years. However, in 2016 we saw a few early signs of what might be termed regulatory 'crossover' or 'convergence' where other regulators, largely anti-trust (competition) authorities, strayed into the data protection arena, and vice-versa. This is largely as a result of the impact of new technologies, such as Big Data and the Internet of Things.

As well as creating the possibility of a company finding itself subject to 'double' regulatory oversight in respect of the same activity or body of regulation, it can be particularly significant where one regulator has greater enforcement powers than the other. This is currently the case between Data Protection Authorities and antitrust authorities although, of course, this will change with the advent of the GDPR.

By way of example, in his report, 'Opinion on coherent enforcement of fundamental rights in the age of big data,' the European Data Protection Supervisor (EDPS) identified the possibility that future machine-learning algorithms may be able to use data to exploit differences in consumers' sensitivities to price, enabling firms to segment the market into individual consumers, charging according to their willingness to pay. Although he is a data protection regulator, the EDPS nonetheless considered it important to call out the possibility of an antitrust issue.

Equally, the text of the GDPR includes some interactions with antitrust law, notably the new 'right to data portability', which enables individuals to require a data controller to 'port' their data to another provider, including a competitor. On the face of it, this is encouraging a more competitive marketplace for the services, whatever they may be – social networking, online subscriptions, etc. The relevant 'privacy' concern being addressed by GDPR is that by legally enabling individuals to move their data from one provider to another (avoiding 'lock-in'), a provider is less likely to be able to impose onerous privacy terms on an individual.

Another area where the GDPR nods strongly in the direction of antitrust law is with regard to the maximum fines that may be imposed by a Data Protection Authority. In order to understand the meaning of 'undertaking' in the context of a 4% of turnover potential fine, a reference is made to EU competition legislation and the relevant case law. (It was widely speculated during the GDPR negotiations that the DPAs were somewhat jealous of the fining powers of their competition chums, and decided to emulate them in the new law).

On the competition side, in 2016 we also saw Germany's competition regulator, the Bundeskartellamt, open an investigation into Facebook's privacy policies. One of the most interesting and, some might say, ambitious aspects of the case is that it is an attempt by the German regulator to rely on a breach (if there is one) of one area of law – data protection – as the basis of a breach of competition law. One might ask why such an issue isn't really the domain of the German data protection authorities?

Just as technology has driven convergence for companies' business models, so it would appear to be starting to drive convergence (or at least overlap) between regulators. The EDPS noted this in his Opinion, along with a call for greater cooperation and coordination amongst regulators going forward. We will be watching carefully for further signs of this in 2017.

5 NIS Directive

Halfway through our list, and it's the Directive on Security of Networks and Information Systems, known as the "NISD". In response to threats of large-scale cyber-attacks which can have a domino effect across industries and countries, last summer the EU adopted its first comprehensive piece of legislation on cybersecurity. Member States have until 9 May 2018 to implement the Directive in their national laws. The UK Government confirmed at the start of 2017 that the UK's implementation will go ahead as planned.

The NISD sets out obligations for two categories of business — and the obligations vary depending on which category you fall into. Firstly, operators of essential services in critical sectors which can be the target of network attacks having a significant impact on society and the economy, such as banking, energy, health and transport. And secondly, key digital businesses, identified as online search engines, online marketplaces, and cloud computing services providers.

The good news for micro and small digital enterprises is that they are specifically exempted from NISD compliance, as are hardware and software developers. Businesses which are already subject to equivalent regulatory regimes are also out of scope.

Organisations which are covered by the NISD will need to bolster the security of their network and information systems. They will also be required to report 'without delay' any major security incidents to national competent authorities or Computer Security Incident Response Teams, which each Member State will have to set up.

Because cyber-attacks rarely occur in isolation and online services have no geographical borders, the NISD also obliges Member States to work together to ensure effective cooperation on cybersecurity incidents and to share information about risks in real time.

Those who are good at counting time will have spotted that the NISD will be applicable just a few weeks after the GDPR. At first glance, there is some obvious overlap between the two texts in terms of data security and incident reporting obligations. Yet, on closer inspection, practical compliance with both sets of rules may cause headaches for businesses. Key differences include the type of interests protected, the scope of data and entities covered, the threshold for incident notification, timing expectations and the audience of disclosure.

Unlike operators of essential services, digital businesses will only be subject to light touch and 'reactive' oversight by national competent authorities. Penalties for non-compliance are left for the individual Member States to determine, so expect to see a degree of variation across the EU.

So, what happens next? Organisations within the scope of the NISD should start reviewing their security and incident reporting standards and procedures. When doing so, they should closely monitor Member States' individual implementations of the NISD, as well as keeping an eye out for Commission guidance on critical open questions such as the definition of affected businesses, the level of security measures required, the criteria for reportable incidents, and any other requirements added on top of the NISD baseline.

4 Surveillance

A reappearance from our 2015 list, the rollercoaster ride that is the UK's surveillance laws, continued in 2016. The Data Retention and Investigatory Powers Act 2014 (known to its friends as "Dripper") was repealed on 30 December 2016 and replaced by the plain old Investigatory Powers Act (known to its enemies as the "Snoopers' Charter").

Despite the removal of "data retention" from its name, the Investigatory Powers Act still contains provisions for the mandatory retention of data by telecoms providers for the purposes of (amongst others) national security, crime prevention, and the regulation of the financial services industry. With the approval of a judge, the Secretary of State can issue a retention notice, ordering one or a group of telecoms providers to retain "communications data" (anything except the meaning of the communication) for up to 12 months. Before issuing the notice, the Secretary of State must take "reasonable steps to consult" the telecoms provider.

In order to access the retained data, a public authority must first obtain a warrant and satisfy the other conditions in the new Act, which vary depending on the type of access being sought. After revelations under FOIA in December that local councils used the old Regulation of Investigatory Powers Act to monitor dog walkers, pigeon feeders and fly tippers, it will be interesting to see how their powers are applied under the new Act — and whether the supposedly strengthened safeguards prove effective.

For the first time, the new Act specifically provides for the acquisition and use of "bulk personal data sets" — that is, the indiscriminate collection of data by GCHQ et al, where the majority of people in the data set will be of no interest or relevance to the investigation. The collection of bulk data sets, which became widely known only after the Snowden revelations, is particularly controversial and was one of the reasons why the new Act had such a tricky legislative journey. Only the intelligence services can access bulk data sets and only for the purposes of national security or fighting serious crime - so local councils shouldn't be able to use them to find people who fail to scoop up after their pets...

Theresa May may have got statute she championed as Home Secretary, but it's not necessarily plain sailing from here on out. Just 22 days after the Act received Royal Assent, the CJEU threw a potential spanner in the works when it released its judgement in the *Tele2 Sverige* case, which concerned the powers of the Swedish telecoms authority and the now repealed DRIPA.

The CJEU held that access by the authorities to traffic and location data could only be justified for the purposes of fighting serious crime, where it is subject to prior review by a court or independent administrative authority, and where there is a requirement that data must only be retained in the UK. The CJEU also took the view that the data retention of this sort should always be the exception, and not the rule. Reading the judgment, it is by no means certain that the new Act would satisfy the CJEU's criteria, suggesting the Act could face a challenge in the UK Courts.

Sitting alongside all of this is Brexit - throwing doubt on the continuing relevance of the CJEU's decisions and Charter rights, whilst also creating concern that the new Investigatory Powers Act may jeopardise the UK's "adequacy" status. One suspects we are not off the rollercoaster yet….

3 e-Privacy Regulation

Just missing out on a spot in our final 2, it's the e-Privacy Regulation. In April, the Commission launched a review of the e-Privacy Directive, the framework which regulates both traditional telecoms providers and various other data-related activities engaged in by most commercial organisations (such as collection of location data, use of cookies and direct marketing). The objective of the review was to ensure the law was fit for purpose, given the technological developments since its last update in 2009, and to align it with the Commission's Digital Single Market strategy and the GDPR.

Whilst some aspects of the existing framework work pretty well (e.g. the regulation of direct marketing), others are much less popular (I'm looking at you, cookie banners). Everyone agrees the e-Privacy Directive needs to be changed; not everyone agrees how.

In July, the Article 29 Working Party and the European Data Protection Supervisor delivered their recommendations on the changes they wanted. These included extending 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), imposing greater obligations to secure confidentiality of communications, and ensuring technology neutral rules for the use of cookies and similar technologies.

However, it became clear from the Commission's consultation that there were some very different views amongst the industry. Many respondents wanted substantial changes to the existing regime (in particular to the cookies rules), and some questioned the need for the complementary legal framework at all — given the comprehensive nature of the GDPR.

The Commission's proposal shed some light on the direction of flight in January. Spoiler alert: it's not the direction many in the industry wanted. Here are a few key points (brace yourself):

- It's a Regulation, which the Commission is ambitiously aiming to come into force on 25 May 2018. We suspect that date is already marked on your calendar so it might just be a case of updating that to-do list.

- The scope has been extended. Firstly, to cover those OTT providers. This means anyone offering chat functionality through their app will now be subject to the new security and confidentiality rules. Secondly, taking after its big brother GDPR, the territorial scope includes non-EU entities providing services to EU users.

- Cookies (and similar technologies) that are necessary to use services, such as single-session cookies used for online form-filling or those used by a provider to analyse its own web traffic, are exempt — but all other cookies need consent.

- On top of that, consent becomes more difficult to obtain, requiring an affirmative action by the user rather than merely passive acceptance once more detailed information has been provided. Users must also be reminded of their ability to withdraw their consent every six months.

- Software providers (including browsers) must also ask users for their privacy preferences (e.g. “never accept” or “always accept”) on first installation, and offer users the ability to prevent third parties storing information. On the plus side (for users at least), by allowing users to centralise their privacy references through browsers, we may start to see at least a reduction in those annoying cookie banners? Here’s hoping...

- Finally, on fines, the draft provides for a maximum of up to 4% or €20 million of global annual turnover for breaches of certain articles and 2% or €10 million for less serious breaches. Sound familiar?

Of course, things may change during the negotiation process — so far, all we’ve seen is the Commission’s proposal. Certainly neither privacy advocates nor businesses seem overly pleased with proposals. 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 GDPR wasn’t enough to worry about...).

Maybe those cookie banners don’t seem that bad now, do they?

2 Brexit

Brexit means Brexit…but what of Data Protexit? We were all busily preparing for the GDPR, and then the EU referendum happened. Amongst all the uncertainty created by the result, we were left wondering what would this mean for UK data protection law? Would we keep the 1998 Act? Would we implement a "GDPR-lite", cherry-picking our favourite bits? Or would we stay in the EEA, meaning in fact we'd keep the whole thing?

So far, it has proved to be a classic case of "Keep Calm and Carry On". As the ICO was quick to point out after the referendum result, any business with establishments in the EU, or which offers goods and services into the EU or monitors individual behaviour in the EU, would be subject to the jurisdiction of the GDPR in any event. The ICO continued to look to the GDPR as its 'best practice' standard. Then in October, the UK Government confirmed that since the UK won't exit until after May 2018, they intend to apply the GDPR in the UK as scheduled.

But it's not true to say Brexit will have no impact on UK data protection law. There are a number of bits of the GDPR which the UK will need to tweak (or abandon?) once it's outside the EU. We don't yet know what the ICO's place will be on the European Data Protection Board, how BCR applications will work, or whether the ICO will have any role in the 'One Stop Shop'. Certainly, organisations whose European headquarters are in the UK are now having to look elsewhere for a 'lead DPA' — and those whose sole European establishment is in the UK may be at risk of losing the benefit of the One Stop Shop altogether.

The other interesting aspect of the UK becoming a 'third country' is data transfers — and this was called out as an area of focus in the Government's Brexit White Paper. There is already intense lobbying going on for the UK Government to secure the UK's "adequacy decision" as part of our exit package (a "Brivacy Shield" anyone?). However, any consideration of adequacy comes with a great deal of nervousness if, in making its decision, the Commission (or indeed the CJEU in a subsequent challenge) decides to examine the UK's surveillance laws. Without the benefit of the Member States' exemption of national security from the EU's remit and in the absence of Charter rights, will the UK's decision to keep the GDPR in full be sufficient to satisfy the Commission?

With so much uncertainty regarding the wider Brexit position, it is impossible to predict precisely what will happen in the arena of data protection. The UK Government may decide to tinker with the GDPR post-Brexit, to make it more business-friendly. During the negotiation of the GDPR, the UK was particularly keen to reduce the administrative burdens on SMEs (e.g. the need to appoint a Data Protection Officer and keep additional records). For most businesses operating across the EU, however, the need for a pan-European model means the GDPR will continue to be the standard to aim for.

1

Coming in at number one...

...International Data Transfers

Possibly because we're all pleased to have a change from poring over the GDPR, we are proud to present international data transfers as our No. 1 issue in data protection and privacy for 2016.

Why so? Well, in response to the events of 2015, 2016 saw the EU Commission, the US Government and others take a proactive approach to calming the choppy waters of international data flows (don't worry, that's the only maritime metaphor). But as with all best laid plans, well, it didn't quite go as intended. Sure, we are no longer seeing headlines heralding "the end of the internet as we know it", but are we really in a more certain place than we were at the end of 2015?

Privacy Shield

First up, the EU-US Privacy Shield Framework. As was to be expected for the framework replacing Safe Harbor, Privacy Shield got off to a shaky start. Published in February, Privacy Shield 1.0 was met with a lukewarm to ice-cold response (depending on who you asked). The Article 29 Working Party acknowledged it was an improvement on Safe Harbor; they welcomed a number of the steps taken by the US government in respect of national security, surveillance and the fundamental rights of EU citizens, including the Judicial Redress Act, representations of the U.S. Office of the Director of National Intelligence and the creation of the role of the Ombudsman to assist EU citizens.

However, there were significant concerns that Privacy Shield did not adequately control the commercial use of data, particularly how long it could be retained and shared with third parties with adequate controls. Privacy Shield's first report card read: "Can do better".

The Commission and the US government took on board these criticisms and published Privacy Shield 2.0. The revised framework tightened controls on businesses' use of data and dealt more expressly with the rights and redress mechanisms of EU citizens. Acknowledging these improvements, a stay of execution was granted by the Working Party pending the first annual joint review in 2017, when the true effectiveness of Privacy Shield can be tested.

Within two months of Privacy Shield being open for business, 400 organisations had signed up and been certified and another 1000 were working their way through the Department of Commerce system (1,390 organisations have certified as

of January 2017). That may not seem particularly high given the significant effort involved in its enactment. However, the list includes some of the largest global organisations, such as Microsoft, Google, Facebook and Amazon. Given Safe Harbor's sluggish start back in 2000, the Commission and the US are counting this as a big win and an endorsement from businesses that Privacy Shield has a future.

Not everyone was feeling quite so generous on the goodwill front however. Within the same two month period, two privacy advocacy groups, Digital Rights Ireland and La Quadrature du Net, challenged the validity of Privacy Shield before the EU's General Court. Specifically, both are seeking an annulment of the Commission's Decision enacting Privacy Shield due to a "manifest error of assessment" by the Commission. It remains to be seen whether either group shall be deemed to have legal standing to challenge the Commission. Meanwhile the Commission is bullish Privacy Shield will live up to the requirements set out by the CJEU in *Schrems* should it come to that. We hope to have some answers towards the end of 2017.

Of course, the big unknown when it comes to Privacy Shield is the Trump factor. The continued support offered by the Commission and the willingness on the part of the Working Party to "wait and see" was in large part due to commitments given by the Obama administration in respect of improving the controls on surveillance activities. Whether this survives the Trump era remains to be seen. Just before our Top 10 went to press, Trump issued an executive order which has the potential to impact on the privacy rights of non-US citizens.

Model Clauses and Schrems vs. Facebook: Part 2

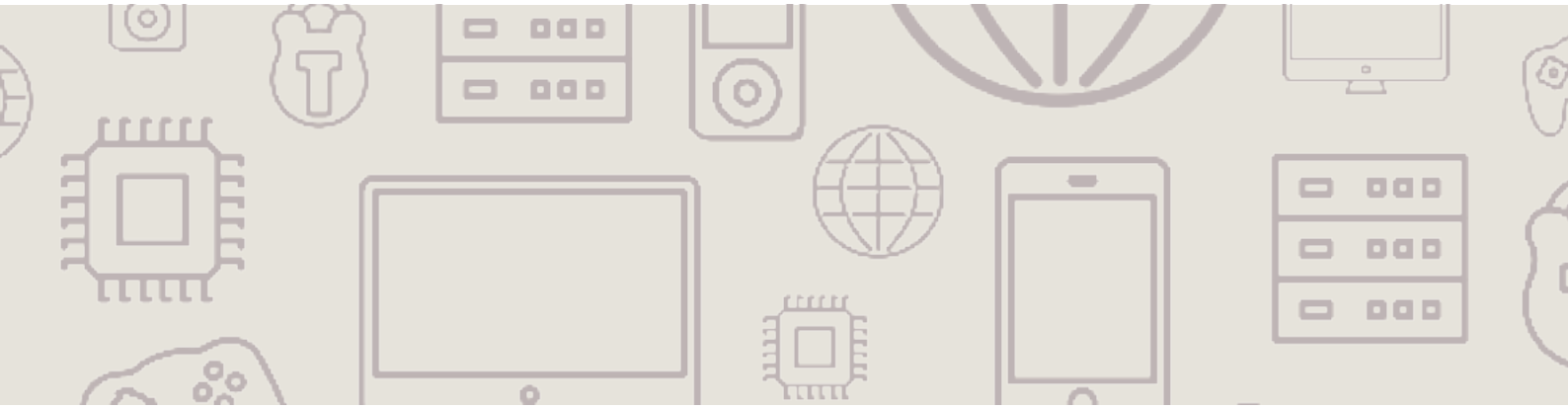
With all that uncertainty, how is that old stalwart of international data transfers, the Model Clauses faring?

Following the CJEU ruling on Safe Harbor, Max Schrems made it clear he wasn't going anywhere and launched a new challenge — this time on Facebook's reliance on the Model Clauses. The Irish Data Protection Commissioner commenced an investigation and took the view that under *Schrems* she is unable to make a determination on the validity of a Commission Decision, including the Decision on which the Model Clauses were based. The Commissioner felt compelled to refer the question of the validity to the CJEU. The Irish High Court hearing to determine whether to make such referral is to be held in February 2017. Watch this space.

The good news for those relying on Model Clauses is that — away from the spotlight of the Schrems vs. Facebook saga — the Commission was busy trying to address any issues with the Model Clauses identified in the *Schrems* judgment.

In the final days of 2016, and with very little fanfare, the Commission adopted Decisions revising (but not replacing) the Model Clauses. In short, the Commission Decisions remove any restrictions on the powers of the Data Protection Authorities to investigate data flows notwithstanding that Model Clauses may be in place, which was a significant concern of the Court of Justice in *Schrems*. The Commission removed similar restrictions contained in the Adequacy Decisions of third countries, as well as adding commitments to conduct reviews of the adequacy of protection periodically.

Importantly all existing Model Clauses remain valid for now (all breathe a collective sigh of relief). However, the revised Decisions should offer those concerned more security than before. We all know that Model Clauses have their limitations, and the changes made by the Commission may lead to Data Protection Authorities taking enforcement action against those blindly relying on Model Clauses. However, some additional peace of mind is exactly what many global businesses have been asking



for since *Schrems*.

What about the General Data Protection Regulation?

Had to sneak it in there somewhere, didn't we? By and large, international data transfers remain the same under GDPR but we are going to squeeze as much positive news out of this topic as possible.

The formal recognition of Binding Corporate Rules in the GDPR and the simplification of the approval process is a welcome development for many global businesses. Hopefully it will encourage the update of this particular transfer mechanism sometimes seen as "not worth the effort".

Looking to the future, Model Clauses, at least as a concept, are firmly here to stay. We expect to see a revised set of "GDPR-proof" Model Clauses in 2017. We also hope to (finally) see Model Clauses for processors in the coming year – particularly given the direct statutory obligation placed on processors under the GDPR to ensure transfers comply.

The Commission has been arguing that the inclusion of codes of conduct and certification mechanisms under GDPR provides businesses with much greater flexibility, particularly those, perhaps, in the technology sector, dealing with Adtech or the Internet of Things. Whether these come to fruition or not as viable mechanisms to enable international transfers will depend on the approach of the Commission and the European Data Protection Board. Both codes of conduct and certification mechanisms need to be approved afterall. We hope that neither will become so onerous for business as a result that they fail to fulfill their potential.

On the whole, we think 2016 has been a pretty positive year for international data transfers. If nothing else, at least we have more certainty than this time last year. Let's hope for more of the same in 2017...

The **2016/17 Data Protection Top 10** was brought to you by...

Robert Bond
robert.bond@bristows.com

Hannah Crowther
hannah.crowther@bristows.com

Neelum Dass
neelum.dass@bristows.com

Alex Dittel
alex.dittel@bristows.com

Robert Fett
robert.fett@bristows.com

Ralph Giles
ralph.giles@bristows.com

Faye Harrison
faye.harrison@bristows.com

Brian Johnston
brian.johnston@bristows.com

Vikram Khurana
vikram.khurana@bristows.com

Emma Macalister Hall
emma.macalisterhall@bristows.com

Christopher Millard
christopher.millard@bristows.com

Laura Peirson
laura.peirson@bristows.com

Rob Powell
rob.powell@bristows.com

Janine Regan
janine.regan@bristows.com

Helen Rose
helen.rose@bristows.com

Sarah Ruthven
sarah.ruthven@bristows.com

Bathilde Waquet
bathilde.waquet@bristows.com

Mark Watts
mark.watts@bristows.com

Sacha Wilson
sacha.wilson@bristows.com

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

#snooping

#privacy

#geek

2

1

#artificalintelligence

6

#nofilter

7

#brexit

#topten

#newentry

8

#privacyshield

#dataprotection

3

5

#hashtag

#nuisancecalls

#bristowscookiejar

#countdown

#spam

9

#selfie

#cookies

#data

#alternativefacts

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.