DATA PROTECTION 2015

TOP 10

BRISTOWS


#rofl
#spam
#privacy
#geek
2
1
#awesome
6
#nofilter
7
#topten
#clickbait
#cookies
10
#newentry
8
#safeharbor
#lolz
3
#dataprotection

#nuisancecalls

5

#hashtag

#likeforlike

Introducing the Data Protection Top 10

We love a good Top 10 here at Bristows – Top 10 films, Top 10 songs, Top 10 lunchtime sandwich fillings – so why not a Top 10 Data Protection issues in 2015? Luckily, 2015 was not short of incidents or a few surprises, making it a busy year for the Bristows Data Protection Team.

What follows is our assessment of the 10 things that mattered most in data protection in 2015 (in order of significance). Of course, it's in the nature of any Top 10 that some of you will disagree. Perhaps you would order things differently. Perhaps you would include something else entirely. That's OK. We won't pretend to have been particularly scientific in our methodology. Our list is the result of considerable discussion, much haggling and, frankly, several glasses of wine. Please enjoy responsibly.

#countdown

#selfie

9

#data

#risingstar

4

DATA PROTECTION 2015 TOP 10

10 Subject access requests

Kicking off our Top 10... We won't pretend it's as dramatic as *Schrems* or the GDPR (all will be revealed...), but there was some news about subject access requests in 2015 which is worth knowing about.

Does it matter why the person made the subject access request that's just landed on your desk? The High Court says yes, it does. Fishing exercises designed to get hold of information for use in litigation aren't what subject access rights are for – there has to be a privacy 'angle'. But, in the *Kololo* case, the court still ordered disclosure of records wanted for use in appeal proceedings. Context counts for a lot, and it made a difference that the man who had made the request was trying to overturn a death sentence.

The Courts also reassured data controllers that there are (some) limits to the lengths that have to be gone to in order to comply with a subject access request. Data controllers will be relieved to know that the Courts draw the line at trawling through 30 years' worth of records, paying for skilled lawyers to analyse each document to weigh up whether it's subject to legal professional privilege, at great cost. The case also gave guidance on lots of other issues about subject access rights and it has been appealed. So keep an eye out for *Dawson-Damer* in the Court of Appeal this year.

The ICO warned us all to watch out for human error and IT problems when responding to subject access requests. The regulator issued (very practical) guidance on redacting third party personal data – beware of hidden worksheets, meta-data and formattable pdfs.

At long, long, last enforced subject access was criminalised. The change in law stops employers from forcing someone to make a subject access request about their criminal past. An employer might hold the prospect of a job over an interviewee to get them to hand over, say, their Police National Computer records. Those records might include 'spent' convictions that shouldn't be taken into account. Instead, employers must use legal criminal record checks operated by the DBS. After languishing on the statute books for 17 years, the provisions finally came into force in 2015.

And what does the new world of the General Data Protection Regulation have in store for subject access rights? The big change is that you won't be able to charge a fee. Okay, the £10 you can charge at the moment barely covered the postage, but most people reckon it's a good deterrent against too many requests. Once SARs are free, will the number surge?

Data controllers will also need to get ready to provide more information. Data subjects will be entitled to know about retention periods, and there's a focus on security concerns over international data transfers. Also, you won't just have to be able to show the Data Protection Authorities that your data transfers are compliant – data subjects will also be able to police this. Under the new regime, data subjects will be entitled to know about international transfers and the safeguards in place to enable them. There's also a broader carve-out aimed at protecting the rights of anyone else who might be affected by disclosure to a data subject – which could mean a delicate balancing act for controllers.

9 Developments in technology

In at No.9, it's technology. Love it or hate it, even the most ardent luddites can't live without it. In a year which saw smart mattresses, smart egg boxes and even a connected Barbie, it's clear that the capabilities of the Internet of Things and Big Data are only in their infancy. Experts reckon there are around 13 billion IoT devices currently in use and this figure is expected to nearly treble by 2020. That's an awful lot of data.

Technology makes a difference to data protection in two ways. Firstly, it means tech companies are collecting data about us pretty much every minute of our lives. And secondly, they are getting so much better at doing things with that data.

One of the main privacy issues for IoT and Big Data is the need to ensure transparency, particularly over the logic involved in the analytics and the various sources of the data. Another challenge is to put end-users in control of their data. Usually, this is achieved by effective rights of access, correction and data portability. Data security is also a major concern in the face of growing cyber threats.

Much ink has been spent on the incompatibility between the traditional data protection principles and the very nature and purpose of IoT devices and Big Data. In response, the GDPR will introduce new requirements intended to address the technological revolution. The new ideas of 'Privacy by Design' and 'Privacy by Default' should help transparency and user control become a reality. We will also see more Privacy Impact Assessments, helping IoT and Big Data businesses make fair and lawful decisions about people's data, such as whether secondary data uses are compatible with people's reasonable expectations, whether they can rely on the 'legitimate interests' condition, and whether the principle of data minimisation is satisfied.

The good news for Big Data and IoT stakeholders is that there may still be room to reduce the impact of data protection laws, depending on your situation. For instance, careful use of appropriate anonymisation techniques may allow the safe use or sharing of data (be careful though – true anonymisation is becoming increasingly difficult). The concept of 'functional separation' may also reduce the privacy impact while at the same time enabling businesses to make secondary uses of the data. Alternatively, use of the data purely for research purposes will carve out a number of data protection requirements under the so-called 'research exemption'.

Privacy issues have kept the tech industry increasingly busy over the year 2015, and there is plenty more to come. If you haven't already done so, take a quick look at the recent Consumer Electronics Show 2016 Conference, held in Las Vegas, which will give you sneak preview of the technologies to look out for this year.

8 Jurisdiction of the Directive

Obviously, there's little point in talking about a law unless you know which ones (if any) apply to you. 2015 saw the territorial scope of the existing Data Protection Directive become yet more complicated, as the continuing fall-out from *Costeja* and the new *Weltimmo* decision made an already tricky issue even trickier.

In *Costeja* (aka the 'right to be forgotten' decision), the CJEU bent over backwards to find that Google, Inc. was 'established' in Spain due to the advertising sales function performed by its Spanish affiliate. In December, the Article 29 Working Party updated their Opinion on Applicable Law in light of *Costeja*. They have jumped on the 'inextricable link' test and are running with it – taking the view that processing 'in the context of' an EU establishment means are the two 'inextricably linked'.

The *Costeja* ruling was in 2014 – but it makes our Top 10 because its impact continued to be felt throughout 2015, not least in the *Weltimmo* decision by the CJEU in October.

Whilst plenty of people were surprised by the Costeja decision, *Weltimmo* couldn't really have gone any other way. The operator of a property website only advertised properties located in Hungary, the website was written exclusively in Hungarian, the owners lived in Hungary, and they had appointed a representative in Hungary. But the company itself was registered in Slovakia, and so the owners tried to claim only Slovakian law applied.

As you'd probably expect, the CJEU disagreed and found the website was subject to Hungarian data protection law. The CJEU decided that the processing of the advertisers' data on the website took place in the context of the activities in Hungary, and that the representative was sufficient to constitute an 'establishment'.

Although maybe very fact-specific, this ruling still had online operators based outside of the EU (but offering services into the EU) reaching for the smelling salts. Following *Costeja* and *Weltimmo*, it's unlikely they can long maintain a stance that EU data protection law does not apply to them.

The upcoming GDPR is intended to clarify the tests for jurisdiction, but whether it does so remains to be seen. For those established in the EU, the test remains the same. But for those outside the EU, the GDPR will apply to a controller or processor offering goods and services to individuals in the EU (with or without payment) or monitoring individuals' behaviour within the EU. This should avoid any further gymnastics by the CJEU with the current 'establishment' test, but it's unlikely to end the judicial wrangling on the topic altogether. No doubt plenty of non-EU operators will ask for clarification on the scope of the new test as they try to resist the 'long arm' of EU data protection law.

7 Civil monetary penalties

Whether it's Schadenfreude or fear for our own organisation, the fines issued by the ICO always make interesting reading.

In 2015 the ICO issued almost 20 Civil Monetary Penalties, an increase on the previous year. There was a particular focus on unsolicited marketing communications, with over half of the fines being for breach of PECR (compared to only a handful in 2014). This shows the effect of the change to the fining threshold in PECR.

The highest fine issued in 2015 was £200,000 – and a CMP for this amount was issued on three separate occasions. Two of the three involved unsolicited marketing communications, the highest amount ever issued for nuisance calls.

The third £200,000 fine was to the Crown Prosecution Service after laptops containing videos of police interviews with victims and witnesses were stolen from a private film studio. Even though the ICO considered that the data was probably not accessed by the thief, the CPS still got fined for failing to take appropriate security measures to protect the data.

One of the big CMP stories of the year was Reactiv Media. Reactiv Media appealed its £50,000 fine for making nuisance calls to people who were registered on the Telephone Preference Service, only to have the First-Tier Tribunal say the fine was too lenient and increase it to £75,000. This is the first time that a CMP fine has been increased on appeal – and I think we can safely say Reactiv Media wish they had paid it right away instead.

2015 was also the year of the lowest CMP, of just £250. It was issued to the Bloomsbury Patient Network after one if its representatives, on two occasions, sent an email to between 60 and 200 people without using Bcc. Because of the nature of the Network's service, receiving the email potentially revealed the recipients' HIV status. The tiny amount of the fine shows the ICO had considerable sympathy for the Network, a not-for-profit unincorporated association – but it still wanted to give them a slap on the wrist.

At the moment, the ICO can only issue fines of up to £500,000 (although it has never actually gone beyond £325,000). But of course, this will all change under the new GDPR. Come 2018, the ICO will be allowed to impose fines of €20 million or 4% of global turnover. This has the potential to be a game-changer for data protection law, elevating it to a similar status to Competition law. Suddenly, the DPAs will have a serious weapon in their armoury, sufficient to make even the largest of global conglomerates sit up and pay attention.

Civil monetary penalties - the year in numbers

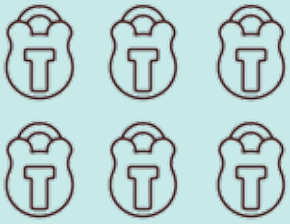
55% of CMPs were for a breach of **PECR**

V

45% were for a breach of the **DPA**

£200,000

The highest fine, issued on **three** occasions



6

MPNs issued where the controller's system had been **hacked**

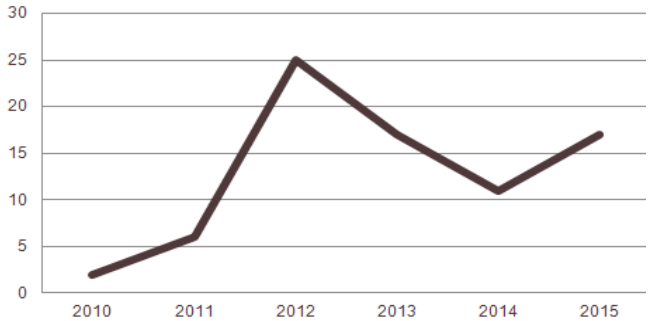
£120,000

The average amount levied in 2015

83% of CMPs were issued to **private** entities

V

17% were issued to **public** authorities



Number of **CMPs** issued since 2010 (**18** were issued last year)

£250

The lowest fine, to Bloomsbury Patient Network

£2,030,250

Total amount levied, compared to £1,152,500 in 2014

6 Cyber security

Confidently striding in at No.6 is cyber security. Web-based attacks increased globally by a whopping 38% in the course of 2015, making cyber security more important than ever to the online economy and customer confidence.

A number of NHS Trusts and local authorities continued to cement their reputation for lamentable data security, with a significant number being slapped with ICO fines. Charitable organisations also came under fire with The Alzheimer's Society and an HIV support service suffering high profile data breaches.

It wasn't just public bodies and charities that hit the headlines, with the growing prevalence of 'hacktivism' (read: do-gooder hackers with a moral objective) keeping the CEOs of large global corporations awake at night.

Unless you spent 2015 under a rock, you couldn't have failed to hear of the Ashley Madison scandal: a group of cyber vigilantes, disapproving of the dating website's mission to promote extra-marital affairs, leaked the personal details of 37 million users. The much-publicised scandal highlighted the challenges that hackers present to the online world and the importance of taking cyber security seriously. Yet not all data breach publicity is bad publicity: if reports are to be believed, Ashley Madison's subscriptions are since on the up...

Sony Pictures was also thrown into the spotlight, when a (supposedly North Korean) hacktivist group leaked racist emails exchanged by one of its co-chairmen, in an attempt to force Sony to scrap its film, 'The Interview', a satirical comedy portraying the assassination of Kim Jong-un.

Another buzz-phrase regularly batted about in 2015 was that of 'front-door attacks'. Though increasingly sophisticated encryption technology is becoming available, individuals and organisations alike remain guilty of using weak passwords, or a single password across multiple services, essentially leaving the 'front-door' open for opportunist hackers. In Ashley Madison, email addresses and passwords were publicised, enabling anyone to try their luck using the same credentials for Facebook, Tinder, you name it. On the flip-side, such data leakage does give savvy organisations the opportunity to scan their systems for identical user details and temporarily block relevant accounts from access.

The continuous increase in security incidents has made cyber security a firm priority for the European Commission. In December 2015 the EU legislative bodies reached agreement on a Network and Information Security Directive, applicable to key industries such as banking, health and energy, though the final text is yet to be approved. The GDPR also has a stronger focus on data security than its predecessor, introducing more prescriptive obligations, including mandatory breach notification.

Looking forward, scandalous data breach revelations will no doubt continue to storm the news in 2016. Hopefully, we will also likely see further progression of the increasing measures to combat them.

5 Surveillance

Half-way through our chart, and it's time for a little snooping. In this post-Snowden era, it'd be impossible to get through a year without new legal developments in the field of surveillance.

With threats to national security rarely out of the news, intelligence agencies are increasingly relying on access to communications data to try to catch the bad guys. But this mass surveillance is highly controversial, and getting the balance right between privacy and security has never been harder. Whether you are a proponent of 'if you have nothing to hide you have nothing to fear', or believe we are on the brink of an Orwellian police state, 2015 threw up plenty to take an interest in...

Firstly, the retention of communications data: the saga continues! Last summer, the High Court found a section of the UK data retention legislation (known as DRIPA) to be incompatible with EU law, after the CJEU had held that the Data Retention Directive was unlawful. The case is currently pending before the Court of Appeal, which referred questions to the CJEU back in November. If the High Court's judgement is upheld by the higher courts DRIPA's sunset, currently scheduled for the end of 2016, will be brought forward to March.

With DRIPA's life coming to an end, the UK government fast-tracked new legislation in November. It's 299 pages long and is called the Investigatory Powers Bill – but is more commonly referred to (at least by the media) as the 'Snoopers' Charter'. It updates and consolidates the legal framework on the use of investigatory powers by UK law enforcement and intelligence agencies. Current proposals include mandatory retention of Internet connection records ('weblogs') for 12 months, potential implementation of encryption backdoors, powers relating to equipment interference, acquisition of data in bulk, and extra-territorial reach. In its current form, the Bill has caused privacy and security concerns amongst most tech companies and privacy advocates. It's too early to tell what the final version of the law will look like, but the key challenge for Parliament will be to ensure that safeguards are in place so that the law can withstand any subsequent legal challenges.

As 2015 drew to a close, the European Court of Human Rights added its own voice to the case law on surveillance. The Court found that a Russian law requiring mobile network operators to install equipments enabling blanket interception of mobile phone communications violated human rights law enshrined in the ECHR. Since the judgement applies to any countries which have ratified the ECHR, including the UK, it may throw yet another spanner in the works of the Investigatory Powers Bill.

So what about 2016? Communication service providers should be on the lookout for the final version of the Bill before it is passed to Parliament. There's also a question mark as to whether the CJEU will be able to deliver its preliminary ruling on DRIPA before the passing of the Bill and the expiration of DRIPA. In the face of constant national security threats, the Government and law enforcement will continue to make the case for surveillance – but first they will have to do a better job convincing opponents that such mass-data gathering really does make the world a safer place.

4 Changes to PECR

At No.4, the changes to the Privacy and Electronic Communications (EC Directive) Regulations 2003 (more snappily known as 'PECR'). For anyone who's ever been bothered by an unwanted call or text trying to sell PPI or double-glazing, this was some good news.

In April last year, the threshold to issue a fine for breach of PECR changed, making it easier for the ICO to clamp down on nuisance calls and texts.

Before the change, the ICO's big problem with PECR was that the fining threshold was the same as for a breach of the Data Protection Act. Before the ICO could go after companies that were responsible for making unsolicited calls, it had to show that those calls caused, or were likely to cause, '*substantial damage or substantial distress*'.

Sure, these calls and texts can be unbelievably irritating, but it's pretty rare that they cause you damage or distress, let alone *substantial* damage or distress. Which meant the ICO was having trouble making its fines stick, and (the ICO felt) unscrupulous marketing companies were getting away scot-free.

Well, the Government heard the ICO's plea and changed PECR in early 2015. The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2015/355 came into force on 6th April 2015, removing the requirement that there had to be substantial damage or distress to issue a monetary penalty.

The ICO will still need to establish that there has been a serious contravention of PECR before it can break out the big guns. However, companies can now face fairly hefty fines - up to £500,000 - if their unwanted calls and texts, in breach of the law, do nothing more than irritate or annoy people.

Armed with stronger powers, it is now much easier for the ICO to take enforcement action against companies who bombard people with nuisance calls. And it has shown no reluctance to do so, issuing nine CMPs for breach of PECR since April.

The new rules don't mean companies can't ever make marketing calls or send texts, provided they do so in compliance with the law. PECR requires consent to send a marketing text and to call individuals registered on the Telephone Preference Service. For individuals not on the TPS, companies should still consider the obligations under the Data Protection Act to provide notice and allow individuals to object to marketing.

3 The rise of the Charter

No one really batted an eyelid in 2009 when the Charter of Fundamental Rights became legally binding. With the Data Protection Directive, a much fuller piece of law already in place, many wondered what, if anything, did Article 8 of the Charter really add?

Hindsight is a wonderful thing. The same question if asked now would get a very different answer. Time and time again, at national and CJEU levels, we have seen the Charter having a profound effect. Article 8 itself doesn't say that much; in terms of wording, it adds nothing to the Directive. But in terms of the status of 'the right to data protection' in Europe, the Charter has given it a massive shot of steroids. That's why it's our No. 3.

One of the first examples was the *Costeja* decision, in which the CJEU used the Charter to effectively read a 'right to be forgotten' into the Data Protection Directive. In 2015 the CJEU showed no signs of rowing back from its 'activist stance'.

Without doubt the most striking example of this was the *Schrems* decision invalidating Safe Harbor.

The *Schrems* decision does pop up later in our top 10, so we won't go into too much detail here. In brief, the CJEU relied heavily on Articles 7 and 8, and Article 47 of the Charter (the right to effective judicial protection) in finding that the Commission's adequacy decision was invalid. Reading the data transfer rules in Article 25 of the Directive in light of the Charter, they couldn't allow the Commission to restrict the powers of the Data Protection Authorities to investigate a complaint from someone regarding an adequacy decision, or allow the Safe Harbor decision itself to stand.

The rise of the Charter is apparent not only in the CJEU's jurisprudence, but also in the national courts. In the UK case of *Vidal Hall et al v Google Inc.*, the Court of Appeal in March last year relied on the Charter to disapply the clear wording in section 13(2) of the UK Data Protection Act 1998, which provided that a person could only claim compensation for distress if they had also suffered damage.

Last but not least, we've seen the impact of the Charter in the retention of communications data. In July, the UK High Court found that sections of DRIPA were incompatible with Articles 7 and 8. As mentioned in No.5 in our Chart, this is currently the subject of a CJEU referral, where it may be another opportunity for the CJEU to champion the rights in the Charter.

All these decisions show an increasing appetite on the part of the courts, both nationally and at an EU level, to rely on the Charter to protect individual privacy – sometimes irrespective of the wording of the statute. It's yet to be seen how the Charter's influence will evolve under the General Data Protection Regulation, but our prediction is that it'll only increase in the coming months and years.

2 The end of Safe Harbor (for now)

There aren't many good data protection jokes, except perhaps the one told in 2011 by the then Polish Data Protection Commissioner. At a conference, he was heard to announce that he didn't like Safe Harbor for the same reason that he didn't like guinea pigs. His problem with these cuddly critters? 'A guinea pig is not actually a guinea, and nor is it a pig, and Safe Harbor is not a Harbor, and nor is it Safe'. In October 2015, we found out he wasn't joking. The CJEU declared Safe Harbor wasn't safe, and could no longer be relied on to transfer EU data to the US.

...And the world came tumbling down.

Well, not quite. The decision has, however, caused significant disruption for pretty much every major IT service provider and online operator with a presence in Europe. The importance of European to US data flows, which are increasing daily, can't be exaggerated. Since the decision, the more than 3,000 US companies registered with Safe Harbor, and thousands more of their EU clients and business partners, have had to rethink their data transfer strategy. For very few organisations has this led to a decision to maintain data in Europe. Instead, organisations have turned to alternative means to safeguard the data – most commonly the EU Model Clauses.

A brief recap of the CJEU's decision: An Austrian student named Max Schrems brought a complaint against Facebook, claiming that its transfer of data to the US on the basis of Safe Harbor was unlawful. The claim was largely prompted by the Snowden revelations regarding the US PRISM project. The Safe Harbor Framework is an agreement between the EU Commission and the US, whereby US companies could self-certify their compliance with certain privacy principles. Under an 'adequacy finding' by the Commission, EU data controllers could lawfully send their data to these certified companies.

In response to a referral from the Irish Courts, the CJEU declared the Commission's adequacy finding invalid. In essence, the CJEU's reasoning was the US legislation surrounding PRISM meant that the US did not satisfy the conditions in the Directive for the Commission to make an adequacy finding. Since the decision, there's been a lot of uncertainty as to what this means for transatlantic data flows in the future. The Data Protection Authorities gave organisations until the end of January to put an alternative legal solution in place, and at the same time reaffirmed the validity of the Model Clauses. But when the January deadline was set, most people thought we would have a new 'Safe Harbor 2.0' – and yet negotiations are still ongoing.

To complicate matters further, certain individual DPAs have expressed doubts about the Model Clauses and Schrems has launched a new challenge of the Model Clauses which Facebook has put in place. The US is in the process of passing the Judicial Redress Act, which gives non-US nationals the right to enforce their privacy rights in US courts – one of the criticisms levelled by the CJEU's Advocate-General. It's hoped that this step will make agreement on Safe Harbor 2.0 easier.

It's clear that, whilst the issue of US law enforcement access continues to be live politically, there will be debate about transfers of data to the US. We must hope that a pragmatic solution is reached sooner rather than later, as the current uncertainty is proving a headache for businesses on both sides of the Atlantic.

1

Coming in at number one...

...no prizes for guessing, it's the General Data Protection Regulation.

After more than three years in the legislative pipeline, three official drafts and countless other leaks and rumours, we have an agreed text. An early Christmas present for those interested in data protection! Once it has been published in the Official Journal of the European Union later in the spring, the 'GDPR' will be applicable across the EU in two years and 20 days time.

The GDPR represents a fundamental change in privacy legislation across the EU, replacing the existing Data Protection Directive from 1995 and (unlike the Directive), applying directly in each member state without the need for national implementing legislation. The significance of this is that, except for certain specific topics where member states are granted discretion by the GDPR, the same statute – not just the same principles – will apply across the whole of the EU.

Now the work of the legislators is over, the work for organisations handling personal data (and of course data protection lawyers!) can really begin. Now we know what the final law will look like (instead of speculating over the drafts), organisations have just over two years to get their data protection ducks in a row.

Before we get into the details of the new text, a quick word of reassurance: although the GDPR is longer than the Directive (200, as opposed to 20 pages), is hugely more detailed, and there are some very significant changes, the 'nuts and bolts' remain the same. We will still have controllers and processors, with the majority of obligations on controllers; the definitions stay broadly the same; and the current principles of fairness, processing grounds, proportionality, data transfers and rights of data subjects still apply.

So what are the changes in the GDPR which make it our number one? And why do these changes matter?

- **Increase in fines.** Probably the most headline-grabbing aspect of the new regime. Admittedly lower than the €100 million proposed by the EU Parliament, the maximum penalties of €20 million or 4% of global turnover (whichever is higher) is still a huge increase on the current thresholds. The fines can be levied against controllers or processors. Of course, we don't know yet how much the Data Protection Authorities will use their new artillery, but the threat of a massive fine will surely get companies sitting up a little straighter whenever data protection compliance is mentioned.

- **Processors are subject to the new regime.** A very significant change for service providers, who have previously only been subject to contractual obligations under a data processing agreement with the controller. These now become direct statutory obligations on both parties, and some obligations apply specifically to processors (e.g. when appointing sub-processors).

- **A new principle of 'accountability'.** For the first time, data protection compliance will not only be about what happens when things go wrong. Organisations will also need to be able to demonstrate they are consistently complying with the GDPR in their ordinary course of business. Essentially, this means organisations will need to have appropriate data protection compliance policies in place.

- **More detailed privacy notices.** A practical step for most organisations over the next two years will be to review their existing privacy policies and data protection statements. The GDPR requires organisations to have in place concise, transparent, clear and easily accessible privacy notices. In comparison to the Directive, however, the GDPR is far more prescriptive as to what this means in practice. These notices must identify the purpose of the processing, the retention periods, state whether the data is encrypted, and identify which processing condition they are relying on.

- **New individual rights.** The rights of subject access and the right to object to marketing continue to apply. However they are joined by an expanded right to erasure (the 'right to be forgotten', albeit somewhat watered down) and a right to data portability, including a right to have the data transmitted directly from controller to controller where this is technically feasible.

- **Mandatory notification of security breaches.** Another much-talked about provision. Unless you are a telecoms operator, mandatory breach notification currently tends to be more of a US concern. Under the GDPR, controllers must notify the DPA without undue delay, and in any event within 72 hours, of a security breach. Individuals should also be informed without undue delay where the incident poses a high risk to their rights and freedoms. Processors have a primary obligation to inform the controller without undue delay.

- **The 'One Stop Shop'.** In the case of processing which is conducted by an organisation's establishments in more than one member state or substantially affects individuals in more than one member state, an organisation will be able deal primarily with one lead DPA in the member state where it has its 'main establishment' (although other DPAs may be consulted as part of any investigation). Note that this one-stop-shop option is not available to controllers or processors whose processing does not take place in the context of an EU establishment.

It is of course impossible to summarise all 91 Articles and 135 Recitals of the new text in this article. There are many other aspects of the new law not discussed above that will impact on organisations large and small, and which may require changes to their processes. We can be sure that the next two years will bring guidance from the DPAs and the Article 29 Working Party (which, under the GDPR, will be reborn as the European Data Protection Board). It should become easier to understand what is expected of organisations as the months go by.

Two years might seem like ages – no point worrying yet. And for those organisations that have an existing compliance programme, it may be. They simply need to evolve their programmes to address the new issues raised by the GDPR.

But for an organisation, especially a large organisation, that hasn't got anything in place already, there will be a lot to do. No need to panic, but developing internal policies and guidance and training programmes takes time, especially in a multinational. There can be a natural 'pace' that has to be found to roll-out change successfully; sometimes things just can't be rushed. So at least kicking off the planning stage of a compliance project now or fairly soon would be a good idea. Prioritise your issues, your risks and your deliverables. Plan your way from now to April 2018.

With so much to do, we're fully expecting the GDPR to be No. 1 next year too, but in the current data protection climate you never really know. (Almost) anything can happen.

Here's a couple that didn't quite make our Top 10...

Processor BCRs

Narrowly missing a spot in the hot Top 10, yet happily worthy of some 'pipped-at-the-post' type recognition, we have Processor Binding Corporate Rules. Perhaps not the sexiest of last years' data protection highlights, and still in their infancy compared to their longer-in-the tooth forefathers (the Controller BCRs), Processor BCRs nonetheless sought to make an impact in 2015, with some limited success.

Processor BCRs were introduced to enable global organisations that process their customers' personal data to make intra-corporate group transfers of this data from within the EEA to elsewhere in the world, in compliance with EU data protection legislation. To help potential adopters get cracking with their Processor BCR applications, the WP29 first issued some guidance back in 2013.

In February 2015, it was announced that First Data Corporation had become the first global organisation to obtain approval of its Processor BCRs, with the ICO acting as the lead authority. A number of other multinationals have followed suit.

In general, however, uptake for Processor BCRs has been rather slow. Cue another data protection landmark in June 2015 with the WP29 releasing updated Processor BCR guidance, to allay concerns raised by potential applicants that relying on the BCRs could allow easy access to the transferred data by law enforcement authorities outside the EEA.

Yet this new guidance failed to spark a sudden flurry of Processor BCR approvals. That said, combined with the demise of Safe Harbor, we may start to see increased uptake over the course of 2016, as global organisations look to alternative mechanisms for satisfying EU data transfer laws.

Drones

Resisting the temptation to make a 'droning on' joke (this is the final article, don't worry), it's still worth mentioning Unmanned Aerial Vehicles – more commonly known as drones. Since drones almost always carry cameras, they are becoming more and more popular for policing, surveillance, and traditional photography. There's inevitably a privacy impact of a tiny machine which can fly above people's heads, without being easily detected, filming everything it sees. The ICO now has a page on its website dedicated to drones, and they were the subject of the Article 29 Working Party's first opinion of 2015.

One of the main problems with drones is letting people know they are being filmed. How can you do this if you're flying 100 metres above them, possibly up to 1km away? Another issue to look out for is proportionality – be careful what you collect and what you do with it.

An interesting CJEU judgment from 2014 (Rynes) held that the 'household exemption' in data protection law didn't apply to capturing CCTV footage of a public space outside someone's home. Not much noise has been made about this judgement, but it would suggest those using drones even in a purely personal capacity still need to worry about data protection law.

The **2015 Data Protection Top 10** was brought to you by...

Hannah Crowther
hannah.crowther@bristows.com

Neelum Dass
neelum.dass@bristows.com

Chloe Dickson
chloe.dickson@bristows.com

Faye Harrison
faye.harrison@bristows.com

Christopher Millard
christopher.millard@bristows.com

Laura Peirson
laura.peirson@bristows.com

Helen Rose
helen.rose@bristows.com

Natasha Simmons
natasha.simmons@bristows.com

Bathilde Wacquet
bathilde.wacquet@bristows.com

Mark Watts
mark.watts@bristows.com

Sacha Wilson
sacha.wilson@bristows.com

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

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.