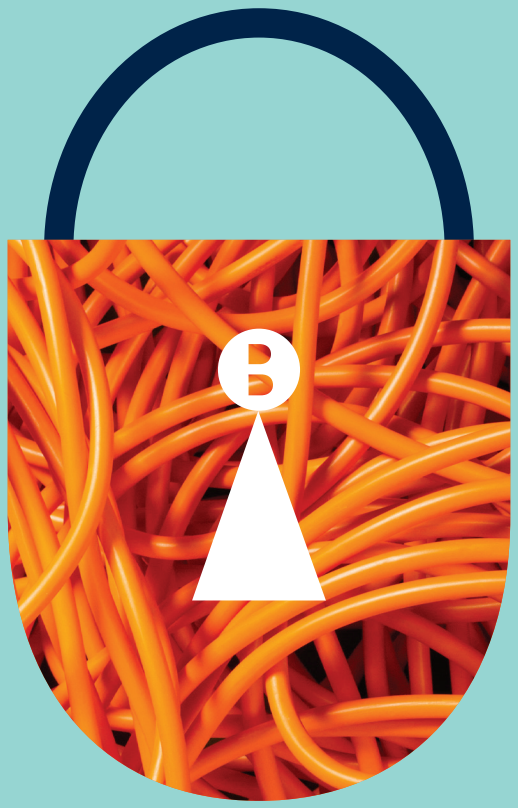
Data Protection Top 10

2018/19



Bristows

GDPR: One year on...

Has it really been a year? (Or maybe you're asking "Has it *only* been a year?!"). 25 May 2018 saw the landscape of data protection law change forever. But on that momentous day, there was still so much we didn't know about how the GDPR would work in practice.

Since then, we've seen implementing national laws, fines, what feels like a constant stream of cyber attacks, long-promised guidance from the regulators, and new data protection laws popping up the world over. We've all learnt a lot.

But there's so much we still don't know. What does a joint controller even mean anymore? Will we ever get an ePrivacy Regulation? And don't get us started on Brexit…

So here it is, Bristows' run down of 10 things we've learnt since 25 May 2018, and 10 things that remain a mystery...

Data Protection 2018/19
Top 10

Contents

10 things we've learnt

1 The sky didn't fall in...

There was a time in the run up to 25 May 2018 when it really felt as if the sky might fall in, and as if the whole world was going GDPR-crazy. High profile US publishers were turning off their websites to EU visitors, a bustling new market for compliance tools had sprung up, data was mapped to the nth degree, company boards were terrified, privacy professionals and data protection authorities were exhausted, and then... nothing happened. No dawn raids. No multi-gazillion Euro fines on day 1. Not only did the sky not fall in, some said GDPR was just a damp squib.

But this isn't the right way to think about it. The sky was never going to fall in. The possibility that it might was, in part, just down to scaremongering, particularly by law firms and consultants, over the size of the likely fines. So the fact that the world didn't end doesn't mean we were wasting our time with all that prep.

Firstly, there has been enforcement action, and there will be more. Complaints were made against several high profile companies on 'GDPR day' itself, one of which led to the CNIL issuing a record-breaking fine. And we're expecting to hear the outcomes of other high profile enforcement actions over the coming months.

And is the number and size of fines really the best measure of the GDPR's impact? Isn't it slightly odd to point to a *lack* of enforcement for non-compliance as a measure of the 'failure' of legislation intended to *promote* compliance? Might it not be better to ask how many more CEOs have heard of data protection now? How many more companies have implemented compliance programmes, and trained their staff for the first time? How many more companies are taking data protection seriously? And have data subjects ever been so aware of their rights? To focus only on a lack of enforcement action is to miss the point.

GDPR is a serious piece of legislation, requiring a serious response, but it was never something for companies to lose all sense of perspective and proportionality over.

2 Life's certainties: death, taxes and data breaches

In the run up to GDPR, the ICO reported a "marked increase" in the number of security incident notifications it had received. To be precise, a total of 957 for Q4 2017/2018. It was really just a sign of things to come. For Q1 2018/2019, the total number of notified incidents was 3,146. For Q2 2018/2019, it was 4,056. That's well in excess of 1,300 per month, 335 per week, 67 per day, nearly 10 per working hour or one every 6 minutes. No wonder the ICO's hotline is occasionally engaged...

It seems hard to believe these large increases are attributable to a dramatic increase in the number of security incidents occurring. Security incidents involving personal data have for some time been an inevitable part of a technological evolution where data has become a valued currency, making it attractive to hackers. However, following GDPR, reporting a security incident is no longer optional where the incident is likely to result in a risk to the rights / freedoms of others.

The ICO's sub-category of reported 'cyber incidents' has also increased dramatically in the post-GDPR world. A significant majority of these cyber incidents involved phishing attacks, which are particularly effective because they target the weakest link in the security chain – the human capacity for error. Other common attack vectors reflected in the reporting involve unauthorised access, ransomware, malware, hardware/software misconfiguration, and brute force password attacks.

It's probably not an overstatement to say that, for many businesses, data security incidents are now a fact of life. In its 2019 Cyber Security Breaches Survey, the Department for DCMS reported that around 32% of business and 22% of charities reported having cyber security breaches or attacks in the preceding 12 months, again with the vast majority being phishing attacks. Clearly, there is something phishy going on. While, oddly, these percentages were down on the previous year's, those businesses that experienced attacks are reported to be experiencing more of them (suggesting that attacks are becoming more targeted), and to be facing greater associated financial costs.

3

The fines are a-comin'...

Surely we all, somewhere in a slide deck or presentation last year, dropped in the phrase "4% of global turnover", the ultimate threat to garner support for our GDPR compliance efforts? So all eyes were on the regulators this year as they started to take their first GDPR enforcement action. Now armed to the teeth with those military grade enforcement powers (the ICO even had SWAT team jackets made), would they be firing off fines from the get go? Or would the pre-GDPR enforcement landscape be left intact?

Well, the message so far is that whilst enforcement efforts have been steadily increasing, with one exception the levels of fines have been broadly consistent with the pre-GDPR world. However, with investigations into some major security breaches ongoing, the coming months are likely to see some further flexing of regulatory muscles.

The headlines were grabbed by the French, with the CNIL issuing Google with an eye-watering fine of €50m for GDPR breaches relating to targeted advertising. In the UK, much of the ICO's focus has been on the use of political data. The fall-out from the Cambridge Analytica scandal has seen the ICO issue its first GDPR enforcement action, requiring Canadian company Aggregate IQ to cease processing UK and EU data for political or advertising purposes. The ICO also issued fines this year (under the pre-GDPR legal framework) for breaches related to the scandal (including a maximum fine of £500,000 against Facebook), and for misuse of personal data during the EU Referendum campaign (including a total of £120,000 against Eldon Insurance and Leave.EU).

The ad tech sector is also in the GDPR firing line. On four separate occasions in the past year the CNIL has taken enforcement action against mobile centric ad tech companies for lack of valid consent mechanisms, in particular in relation to the use of location data. The ICO has also said that web and cross device tracking for marketing is a regulatory priority for the coming year.

Elsewhere, the German, Austrian, Portuguese and Polish regulators have issued their first GDPR fines (the highest of which was €400,000) for a range of breaches including those related to security, transparency and data minimization.

So, whilst regulators are not issuing huge fines as a matter of course, enforcement efforts are intensifying. But it's still too early to tell whether those pre-GDPR warnings were fully justified.

4

Schrems isn't going anywhere...

In these dark times of overwhelming political uncertainty, something we could all use right now is a hero. One man has positioned himself as the data protection saviour of our age, ready to liberate us from the tech giants one complaint at a time. That's right, Schrems is still here, and he's as hungry for privacy justice as ever...

Max Schrems is best known for his eponymous pieces of litigation against Facebook, which have had a wide-reaching impact on data transfers (more on that in our 'still a mystery' pages). But if you think having two game-changing cases under his belt (one of which is ongoing) would keep Max occupied, you'd be underestimating him. Now he's set up a non-profit organisation, NOYB (or 'None of Your Business'), and he's got a whole range of new targets.

Not one to be accused of tardiness, Schrems scheduled the first NOYB action for GDPR day itself, and on 25 May 2018 four complaints were filed against Google, Instagram, WhatsApp and Facebook in France, Belgium, Germany and Austria (respectively). All focused on the issue of consent, presenting various arguments that the consent these organisations rely upon to provide their services is not 'freely given' and therefore invalid under the GDPR; additional arguments claimed that the companies' consent is not sufficiently specific, is too hidden within privacy policies and terms of use, and that in some circumstances the legal basis relied upon is unclear. The consequences so far?

In January, the French authority hit Google with a €50 million data protection fine following an investigation sparked by this complaint and another from a different organisation. What will result from the other complaints is still TBC...

While these first complaints grabbed the headlines, it's not all NOYB have been up to – in January, they filed ten complaints with the Austrian data protection authority against eight media streaming companies (including Amazon Prime, Apple Music, Netflix and Spotify). This time, it's the right to access that's at the heart of their mission, as having made access requests to each company, NOYB allege that none responded in a GDPR-compliant way. NOYB's website also claims that other projects are in the pipeline, but these plans are top secret for the moment. One thing's for certain though, and it's an easy thing to add to our list: Schrems isn't going anywhere...

5 The rise of the class action

"Have you been involved in a data breach that wasn't your fault? Did you know you could be due thousands of pounds of compensation? Call 0800-111-GDPR now!"

Whilst our friends at the ICO could have something to say about this type of nuisance call, it might just be a glimpse of the future as the GDPR looks set to give rise to an increase in US-style class actions.

The GDPR gives individuals the right to claim compensation for non-material damage suffered after a breach. In the UK this had already been the case following a 2015 Court of Appeal decision, but the GDPR confirms that individuals across Europe can claim compensation for "distress".

In addition, Article 80 of the GDPR allows individuals to mandate a representative body to issue complaints and bring compensation claims on their behalf. There are a few hurdles to overcome here, primarily that the representative body must be not-for-profit and have "statutory objectives which are in the public interest". This would seem to rule out bodies established purely to bring a class action backed by litigation funders expecting to make a tidy profit. Nonetheless, we are starting to see Article 80 being exercised in the context of *regulatory* action (for example, the complaint made against Google to the CNIL by NOYB), and its use for litigation may not be far behind.

In the UK, the case of *Various Claimants v WM Morrisons Supermarkets* demonstrates the viability of post-breach follow-on damages claims. The Court of Appeal found that the supermarket chain Morrisons was vicariously liable for the actions of one of its employees who unlawfully uploaded staff payroll data online, notwithstanding the fact that the supermarket ceased to be a data controller at the point at which the employee made the unlawful copy. Whilst Morrisons is appealing the case to the Supreme Court, if unsuccessful it faces paying out compensation to over 5,000 claimants.

What is needed for a successful class action and to make costs worthwhile is critical mass in terms of the size of the class and the potential damages involved. Therefore, as regulators start to issue their first set of fines for GDPR data breaches, and more importantly issue public findings of controller non-compliance, claimants will be watching closely to determine if a particular game is worth the candle. Even as we wait for the final regulatory decisions, we have seen class actions issued or threatened against Marriott Hotels, British Airways and TicketMaster following recent security breaches.

Whatever the outcome of this initial round of claims, it's likely that group litigation is going to be a common feature of data breach fall-out, and businesses should factor this in when assessing risk and apportioning liability with third parties. As the ambulance chasers descend, be prepared!

6 *"I know my fundamental rights and freedoms!"*

Remember the Great Email Flood of May 2018? The countless requests to 're-consent'? The GDPR brought privacy firmly into the public's inboxes, and consciousness. As a result, people have become more aware of their data protection rights – and it's become clear they're not afraid to exercise them.

Requests to access and delete personal data (rights which both existed pre-GDPR) are on the rise. For organisations facing an employment or customer dispute, access requests are increasingly submitted as a backdoor to disclosure. The desire to find that smoking gun / what their employer really thought of them continues to be a key driver. Individuals are also trying out their new "right to be forgotten" or "right to erasure"...sometimes not entirely logically. We've seen organisations receive requests to erase existing customers whilst the services they provide are still ongoing, and even a request to 'forget' a current employee ("And what address would you like your P45 sent to...?")

But whilst people are enthusiastic about asserting their privacy rights, some data subjects seem unaware that the rights are not absolute. A controller's legal basis and its specific purposes for processing personal data are critical in determining whether a request can be granted, and of course there are exemptions which can be relied upon to bring data out of scope.

One year in and it's clear that handling, responding to, and granting individual rights requests are placing an increasing burden on organisations. Access requests in particular can soak up hours of manpower and resources, sifting through unstructured data recovered as a result of email searches. This has seen many organisations asking to what lengths they must go to provide unstructured data. The *"disproportionate effort"* exemption has been axed, but there is yet to be clear guidance on when the *"manifestly unfounded or excessive"* carve-out can be relied on in practice. Rights of the individual vs. burden on the controller, it will be one to watch.

7

The GDPR has *very* long arms

In the months preceding May 2018, a number of website operators outside the EU became increasingly nervous about this new European law they'd heard about, that apparently had worldwide effect. Provided your website could be accessed in the EU, you could (would immediately!) be fined 4% of your global turnover. A number of websites went so far as to block EU users from their site, leaving some EU fans of US news to wonder whether their GDPR protections were worth the sacrifice.

Unfortunately, the European Data Protection Board's (EDPB) Guidelines on the territorial scope of the GDPR, released for consultation in November 2018, did little to abate those concerns. The EDPB insists (amongst other things) that online tracking of EU visitors to a foreign website would be sufficient to trigger GDPR. Moreover, unlike the "goods and services" test, there does not need to be any *intention* to monitor EU data subjects in particular. Provided you intend to monitor someone, and you chance upon someone in the EU, they'll be protected by GDPR.

The EDPB takes a similarly expansive view when it comes to controllers and processors processing in the context of an EU establishment (and so caught by Article 3(1)). The Guidelines state that, where a controller or processor satisfies the "establishment" test, all of its personal data processing is in scope of the GDPR, regardless of the location of the data subjects. This means that individuals in the US, Australia, or even Papua New Guinea, will have the full benefit of GDPR when their personal data is processed in the context of an EU establishment. The EDPB is also clear that the GDPR can apply to processors even when it does *not apply* to their controller – and so all EU processors should offer GDPR compliant terms, even when contracting with non-EU controllers. How much supervisory authorities will spend time and (presumably taxpayers') resources on protecting the rights of non-EU residents remains to be seen.

The Guidelines are still in the 'consultation stage', and so may change. However, they show a clear appetite on the part of the supervisory authorities to ensure that as many people as possible – both inside and outside the EU – have the benefit of the privacy rights the GDPR affords.

8

DPIAs – not such a risky business?

As we all know, the GDPR made it a requirement for controllers to carry out a Data Protection Impact Assessment (DPIA) before commencing processing which "is likely to result in a *high* risk" to individuals, particularly when using new technologies. In the last year, we have got a much better idea of when this might be, as the supervisory authorities published their own lists of 'high risk' processing triggering a DPIA. These national lists were sent to the EDPB to review, and the good news is that not as much as you might think is considered 'high risk'.

At the time of writing, the EDPB has published Opinions on lists from 30 out of the 31 EEA countries (all except Cyprus). In these Opinions, the EDPB actually took a surprisingly narrow approach, identifying numerous processing activities which, in its view, are not high risk on their own, but only if one other risk criteria is present. These include processing biometric and genetic data, location data, and the 'invisible processing' proposed by the ICO. The EDPB also suggested some criteria proposed by the supervisory authorities were not high risk triggers at all, such as Internet of Things, re-using personal data, and joint controllership. The supervisory authorities were told to amend their lists to reflect the EDPB's view, which the ICO has done.

As an example of how to apply these criteria in practice, let's consider geolocation devices being used in the UK. The use of simple wristband trackers by a paintball company with three venues (to add an extra dimension of tracking the opposing team during a match) would be unlikely to require a DPIA: even though geolocation data is used, the processing is on a relatively small scale, and no other risk criteria are met. By contrast, a dating app which matches individuals by approximate geolocation is going to be combining location data with sexual orientation (i.e. special category) data and potentially on a large scale. It therefore ticks off geolocation, special category data and – assuming the app is a success – large scale processing, and so would trigger a DPIA.

Of course there's no harm in doing a DPIA even when it's not required but, for those organisations struggling with the increased compliance burden of GDPR, it's nice to have the load lightened a little. It's also reassuring to see the EDPB placing an emphasis on consistency at a European level, so that multinationals don't have to apply a lowest common denominator approach to DPIAs. This is one successful example of the GDPR's increased harmonisation.

9

Data protection – not as obvious as you might think

One by-product of all the publicity surrounding GDPR was that as well as there being a lot of understanding, there was a lot of misunderstanding, sometimes comically so. Here are a few of our favourites:

- Are window cleaners data processors? Professional window cleaners are often on the outsides of office buildings, looking in, potentially with sight of any personal data on the screens of those working there. Are hairdressers data processors – they do hear a lot of personal gossip?
- If I get a surprise birthday cake for someone ('Happy Birthday Mark!'), do I need to get the person's prior written consent? And should the cake shop ask to see it before icing the cake?
- Are we still allowed to phone the people who we do business with? We've known some of them personally for more than twenty years. Is it true we're not allowed to call them anymore because of GDPR?
- Do we need to delete all our data if we don't have everyone's consent?

Hopefully you don't need us to answer any of these….

10

The GDPR is catching!

Supporters of the GDPR like to say that Europe is a world leader in privacy regulation, but there's always been another body of opinion which complains about overbroad definitions of personal data, and onerous requirements around collection and use of personal data. Proponents of this view have tended to be supporters of the American approach of limited, sector specific legislation. So where is global privacy headed? Is the EU a world leader only in the sense that we are way out in front because no one else wants to follow us? At first glance a look at laws round the world, and recent changes, suggests this is not the case.

In 2018 Brazil enacted a General Personal Data Protection Act, which is largely inspired by and aligned to the GDPR. Japan announced supplementary rules which would apply to European personal data, leading to it being approved as providing adequate protection by the European Commission. India has published a draft Data Protection Bill and, although its authors claim to be rejecting the European model and creating "a fourth way", there is much which would be familiar to a European lawyer, including fines of up to 2% or 4% of a company's worldwide turnover, depending on whether a company is a "significant" data fiduciary. One can't imagine how they came up with those numbers. Both Brazil and India provide for their laws to have extra-territorial effect, and more concerning for many multi-nationals will be the provisions in the draft Indian bill concerning data localisation.

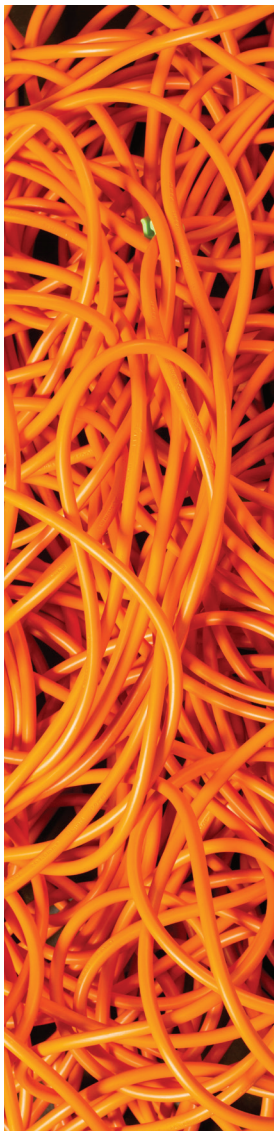
According to the committee of experts which produced the Indian draft Data Protection Bill, 67 out of 120 countries outside Europe largely adopt the framework of the GDPR or its predecessor, the Data Protection Directive. So it look as if privacy is going Europe's way.

But in 2018 a potential game changer emerged from nowhere: the California Consumer Privacy Act (CCPA), a "consumer" protection measure whose approach is distinct from GDPR. The extraordinary story of how the CCPA came to be passed has "film" written all over it (not that the film on the making of GDPR wasn't exciting; if you missed David Bernet's documentary 'Democracy' first time round, it's worth tracking down) but the CCPA is important for reasons other than its cinematic potential. It represents the first time a US state has had a general data privacy law, and, as we've seen with breach notification, where California leads, other states (eventually) follow. More significantly, it has also pushed tech companies into advocating for the first time for a federal privacy law to provide a "consistent, uniform framework" and stop "inconsistent protections for consumers". A law which, coincidentally, could pre-empt the CCPA and the strong consumer protections already embodied within it. Given that the draft GDPR was one of the most heavily lobbied regulations in EU history (with almost 4,000 amendments proposed), congressional lobbyists will be looking forward to a bumper few years.

A year in numbers...

103

monetary penalties issued in 2018 for failure to pay the ICO's registration fee



5,518

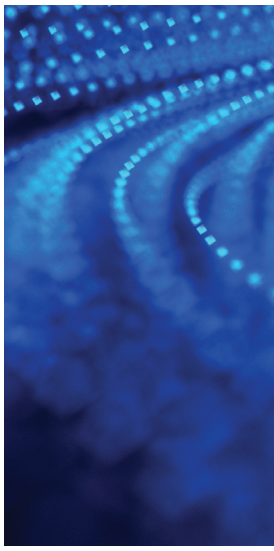
claimants in the group litigation against Morrisons for vicarious liability for the acts of an employee

1,792

breaches reported to the ICO in June 2018 (compared to 657 in May, and 367 in April)

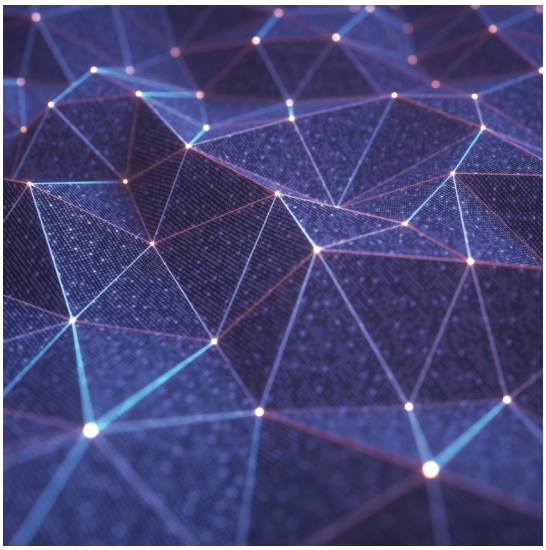
€55,955,871

total fines (as at February)



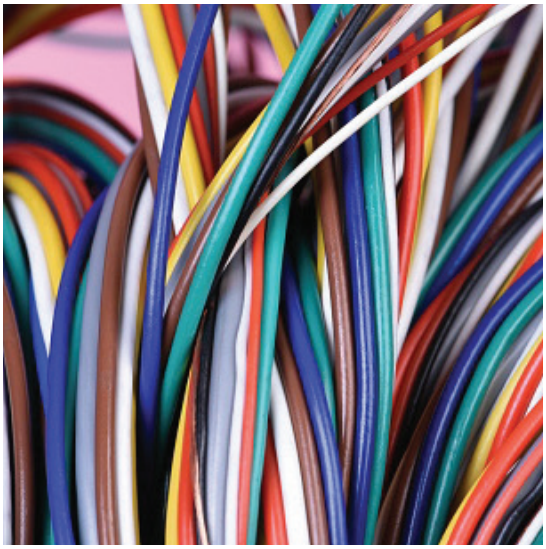
0

fines issued by the ICO under the GDPR, 29 issued under the 1998 Act and PECR



12

Member States have issued fines



1

adequacy decision, to Japan in January 2019

10 things that remain a mystery

1 Data transfers – will the fun never stop?

The best that can be said for the future of the EU's personal data transfers regime seems to be: 'no news is good news'. That's if you're an optimist. There are plenty of challenges before the courts which appear to be moving at a glacial pace, but with no obvious alternatives on the horizon just yet. In short, the future for the critical area of data transfers involves a lot of wait-and-see. In no particular order:

Schrems II: January 2019 saw the hearing of Facebook's appeal to the Supreme Court of Ireland, seeking to stay the reference by the Irish High Court to the CJEU of its questions on the Standard Contractual Clauses. No decision has, at the time of writing, been handed down by the Supreme Court. Meanwhile, the CJEU reference is pending, rather than stayed, with various parties, including Facebook, having filed submissions in the CJEU proceedings. So while we're not ready to write off the Standard Contractual Clauses just yet – with the drastic narrowing of legal options that this would entail for organisations wishing to transfer data globally – we remain in a state of limbo as to their fate.

As to the Standard Contractual Clauses themselves, we're all still rubbing along with the old ones long after the entry into force of GDPR, instead of shiny new ones adopting the changes required by GDPR, with no news from any official source as to when new Clauses are going to be introduced by the Commission.

Meanwhile, the challenge to the EU-US Privacy Shield before the CJEU brought by the French digital rights activist group, La Quadrature du Net, hasn't actually gone away (although there is still no date set for a hearing). To recap, the substance of the claim is that the US ombudsperson, who is responsible for handling EU complaints about surveillance in the US, is not an effective mechanism and lacks sufficient independence, and the claimants are seeking to annul the Commission's Adequacy Decision. Watch this space.

But wait, surely there's a bright new dawn in the shape of those codes of conduct and certification schemes under GDPR, which promised a more innovative future for many areas of data protection compliance, including EU data transfers? After various public consultations by the EDPB on codes of conduct and schemes generally, the EDPB is now considering a consultation on the use of such codes for international transfers, which sounds promising. Turns out so far, however, that enthusiasm amongst interested parties for codes and schemes generally (not just for international transfers) appears less than overflowing: at the time of writing, the public registers maintained by the EDPB both for approved codes of conduct and certification schemes remain……..completely blank.

Does that mean this is BCRs' moment? Sort of – there's certainly a lot of interest, but they're probably never going to be the new normal for international data transfers, except for larger groups of companies.

As to where we'll be in another year's time? Definitely one for our mystery list.

2

Joint Controllers

The last year has seen an explosion in the number of controllers identifying as "joint controllers", due to three cases decided by the CJEU in 2018.

First we had the Facebook Fan Page case, *Wirtschaftsakademie*. The CJEU held that the Facebook fan page owner should be considered a joint controller with Facebook despite not having any access to the personal data, collected via the cookies, which was used for statistical analysis. This was because the page owner was able *"to influence the specific way in which that tool is put to use...designating the categories of people whose personal data will be collected by Facebook"*. The Court also held that joint controllers did not necessarily have equal levels of responsibility depending on the circumstances of the case.

The Finnish Jehovah's Witness case, *Tietosuojavaltuutettu* (help with pronunciation most welcome) followed shortly after, in which the CJEU decided that the Jehovah's Witness community as a whole was a joint controller with a group of door-to-door preachers from that community, because the preaching was *"organised, co-ordinated and encouraged"* by that community. Again, the Court held that the existence of joint responsibility did not necessarily imply equal responsibility of the various operators.

Finally, the Facebook Like Button Case, *Fashion ID*: in this case the Advocate General ("AG") has opined that a fashion retailer which had embedded a Facebook "like" button on its website is a joint controller with Facebook, as it could be said to be co-determining the parameters of the data collected by the simple act of embedding the plug-in at issue in its website. However the AG did at least recognise the difficulties arising from the increasingly broad definition of "controller", including an increased risk for data subjects if it is not clear which controller is responsible for meeting which obligation in a situation where arguably too many parties involved in the processing meet the definition of "controller". In what would be a move away from the position in the previous two cases if followed by the Court, the AG suggested that rather than different responsibility levels, it was better to think of controllers having responsibility for different stages of the processing; i.e. only those they are involved in. So not, in fact, joint after all.

The upshot of all of this is that it's seemingly difficult to avoid a relationship of joint control, in circumstances where previously we might have used the term "controllers in common", independent controllers – or not controllers at all. Given the potential for joint liability under Article 82 of the GDPR, this does not seem an altogether attractive prospect. To (mis)quote the immortal words of Destiny's Child: "all you controllers, who independent, throw your hands up at me..."

3 The ePrivacy Regulation – Season 3

Back for a third season, the draft ePrivacy Regulation is progressing like a drawn-out TV saga. But with such important changes to the online tracking and advertising landscapes, it's hard to stop watching this one. The draft Regulation will replace the existing ePrivacy Directive, bringing the rules up-to-date with technology and theoretically creating a single European standard.

Previously on the draft ePrivacy Regulation...

It's been over a year since the European Parliament issued their draft, and the Council has yet to agree a common proposal. The most recent amendments by the Romanian Presidency to the draft proposal were published in March 2019. On assuming office, Romania was very cautious in setting out the road ahead for the Regulation, preferring to commit to progress rather than a final draft. At the time of writing it's looking increasingly likely that an acceptable position will not be reached before the Parliamentary elections in May. Should this be the case, the LIBE Committee's position may be reopened under the new Parliament and it will be the job of the incoming Finnish Presidency in July to find common ground. So with a final position not yet available, what are the Regulation's most hotly debated issues?

As a possible solution to the consent fatigue issue, the first draft of the Regulation gave individuals' increased ability to control what cookies and similar tracking technologies they receive using their browser settings. Perhaps due to industry lobbying, the Council has proposed this only be a recommendation in the Recitals, at significant odds with the LIBE Committee's view.

The Council has specifically authorised tracking walls (where website access is conditioned on consent to tracking) in the Regulation's Recitals, provided users have a choice of an "equivalent offer". Whether an equivalent offer includes a paid version of the service remains to be seen. In any event, expect pro-privacy lobbyists to fight this change.

The question of whether business-to-business marketing should follow the same rules as business-to-consumer marketing looks likely to be given to Member States. However, there is some opposition to the disharmony resulting from different local applications of the rules, especially where businesses increasingly operate across multiple Member States.

Next time on the draft ePrivacy Regulation...

Some expect the Trilogue negotiations (where the Commission, Council and Parliament thrash out the final form) to begin later this year, meaning that the Regulation could be agreed by the year end leading to a late 2020 application date – provided there is a 12, and not 24, month implementation period (the latter having been suggested by the Council). In the meantime, the potentially giant fines for a breach of the Regulation's provisions will be enough to keep eyes glued to this saga.

4 Controllers v Processors: Whose fault is it anyway?

One year on and we're all still busily allocating liability in our processing agreements largely in the dark. Sure, the ICO has published its guidance on contracts and liabilities between controllers and processors but, truth be told, it won't get you very far. The lack of detailed guidance, relevant precedent and (dare we mention it) standard clauses and certification schemes when it comes to controller/processor clauses means we still don't have answers to some of the big questions around liability under the GDPR.

Looking first at liability for administrative fines: it's standard to see each party limiting and capping its liability to the other for administrative fines under Article 83. However, these provisions may be of limited use given that supervisory authorities will issue fines against the party at fault (i.e. the one who breached the law). Similarly, where these liabilities are covered by an indemnity, there are questions as to whether, as a matter of law, the party at fault will be able to recover its losses under the indemnity.

How about liability for data subject claims? We don't really know how data subject claims under Article 82 will work in practice. How high will the bar be set for processors and controllers relying on the *"proves that it is not in any way responsible . . ."* defence under Article 82(3)? Does this really mean that a party with only a very minor degree of responsibility will still carry joint and several liability for the entire damage of a claim, where there is a controller or processor counterparty who is otherwise entirely to blame for it? And what quantum of damages will the courts determine as being *"full and effective compensation"* in the context of, say, a group claim, where the claimants have suffered distress, but not financial losses?

Lastly, looking at liability for contractual breaches: negotiating Article 28 processing clauses can still be a headache. In particular, determining what the scope of the appropriate technical and organisational security measures are, and which party is liable under the contract for deciding whether they are appropriate, is a bunfight in most negotiations and one that it would be helpful to have some official guidance to fall back on.

So when it comes to liability and processing clauses, all we can do as practitioners is keep on trucking, hope that not too many negotiations feel like Groundhog Day, and look forward to a time when some judicial light shines down to help us on our way.

5 Brexit (sorry)

That boring relative at the party who nobody wanted to invite is STILL HERE – yes, the impact of Brexit remains very much a mystery.

As to where exactly it has got to, it seems that, at least at the time of writing, we're set to hang in there until Hallowe'en 2019. In relation to the specific data protection implications of the process, the last year has seen: technical papers on the topic from our government; more House of Commons committee hearings; a series of speeches by both the EU and UK setting out, inter alia, their 'red lines' on data protection; relevant provisions on the issue in the Withdrawal Agreement and accompanying Political Declaration; draft withdrawal legislation; and – of course – fines from the ICO against Vote Leave for contravention of the law by sending out thousands of unsolicited text messages in the run up to the referendum itself.

For those of you struggling with how best to navigate all these considerations, or who simply think it's silly that if at first you don't succeed, then you should try, try, try, and perhaps, fourth time lucky, try again, here are the headlines:

Brexit and the EU

Most continue to agree that the best outcome for transfers to the EU post exit would be an adequacy decision from the European Commission, as this would minimise restrictions on cross-border data sharing, on the basis that the UK's standard of data protection would be considered 'essentially equivalent' to the EU's. The alternatives (model clauses, BCRs, certification mechanisms, etc) are generally recognised to be a burden on organisations, particularly on smaller organisations. In addition to the benefits for commercial organisations, similar formal arrangements would be necessary for the UK to be able to share data with the EU for law enforcement purposes.

The UK government, however, would like adequacy to be a two-way agreement, in the form of an international treaty. This is a problem for the EU, which does not want to share its regulatory autonomy with a third country and so wants an adequacy decision and not a treaty. In any event, the adequacy procedure can start only once we leave, meaning continuing uncertainty about what will happen to UK-EU transfers. Assuming, however, we get adequacy, if there's one thing that the experience of Schrems I and II have taught us, it's that we can no longer take for granted the status quo. Our position as an adequate 'third country' would be under continuing scrutiny with no guarantee that it would withstand any challenges.

Meanwhile, as part of its contingency planning for the continuing possibility of a 'no deal' exit, DCMS' draft regulations preserve EU GDPR standards in domestic law, recognise EU member states and other EEA countries as adequate to allow continuing data flows from the UK to Europe (on a transitional basis), recognise model clauses in UK law and give the ICO power to issue new ones, and recognise BCRs authorised before exit. Questions abound. In what form might the ICO continue to participate in the EDPB? (Spoiler: in a very limited way, if the EU gets its way on its cherished principle of regulatory autonomy of the EU). And what about any continuing participation in the One Stop Shop?

Brexit and wider transfers, including with the US

The same draft regulations preserve the effect of existing EU adequacy decisions (on a transitional basis). But will the third countries in question maintain unrestricted data flows to the UK? This seems generally to be in their interest, but at the time of writing we are still waiting for some of them to affirm formally that they will do so. As far as the EU-US Privacy Shield is concerned, are we heading for a UK-US equivalent like the Swiss arrangement? Or will the UK instead seek to handle data protection matters as part of the trade agreements that we must seek once we leave?

One constant amidst all the uncertainty remains the importance of personal data in our trade and security co-operation not only with the EU but also with the rest of the world. The best approach is to continue to do all we can contractually to minimise the disruption that Brexit is likely to cause and to hope that negotiations with the EU start to proceed more effectively, or, if not, that that boring relative actually leaves (we're family, aren't we?).

6 How does the One Stop Shop work? (Does it work at all?)

According to the EDPB's report to the European Parliament on the implementation of the GDPR in March 2019, there have been 45 cases launched via the new 'One Stop Shop' (OSS) procedure, with six having been finally concluded. On the face of it, then, it looks like it's all going according to plan. We suspect the reality, however, is not so simple.

In fact, there are so many unanswered questions as to how the OSS works in practice, it's hard to know where to start. One question which has huge significance, however, is who is actually entitled to it? The view which has been adopted by at least some of the supervisory authorities – most notably CNIL in its action against Google – is that the 'main establishment' required for a lead supervisory authority must be, in fact, the *data controller* itself, and not merely "an establishment of" the data controller.

Under this school of thought, organisations headquartered outside the EU, even if they have a strong physical presence in the EU, will not be entitled to the OSS unless they can show the actual decisions as to the purposes and means of processing are made in the EU. Taking account of the fact that, once (if!) the UK leaves the EU, having a controller in the UK will not help, then to avoid the potential of multiple investigations and multiple fines, there may be a lot of multinationals scrabbling around to find a real-life bona fide data controller in the EU27.

It's not clear why the supervisory authorities have taken this view, except perhaps to narrow the situations when the OSS will apply, and thereby retain more scope to start independent investigations. The fact that this appears to directly contradict the WP29 Opinion on appointing a lead supervisory authority (which suggests that *"the pragmatic way to deal with this would be for the company to designate the establishment that will act as its main establishment..."*) does not help with the uncertainty.

Another question which regularly has us scratching our heads is the question of applicable law and jurisdiction in the OSS process. Just like man, the GDPR is not, we must remember, an island: it is inseparable from the Member States' national laws filling in all the tweaks, twiddles and derogations. Some of these allow for substantial divergence, such as the age of consent or the exemptions to the rights.

So when a 'lead' authority takes a case, whose national law applies? Only their own? The Member State where the complaint was made? Both? All 28? But then if the supervisory authorities are right, and the main establishment must be the controller, how can it even be subject to more than one Member State's national law? And if I appeal a decision made by the OSS to my national courts, whose law does the court apply...?

Answers on the back of a postcard please.

7 The Gordian Knot of AdTech and GDPR

"AdTech" (and the breadth of technology that this term encompasses) inherently relies on personal data. The collection of vast data sets, their enrichment and matching are fundamental to an industry which continues to grow at breakneck speed. It's unsurprising then that the GDPR has had, and continues to have, a significant impact on businesses at all levels of the complex AdTech ecosystem. The various players have watched the GDPR's implementation very closely, attempting to create a new industry "normal" where currently uncertainty and confusion reign supreme.

The debate as to whether "GDPR standard" consent can ever truly be obtained in an AdTech context rumbles on. How can the average internet user truly give specific, informed consent to the multiple purposes for which their data is used and the numerous parties it will be shared with? All this achieved by a one-line cookie banner, when many experts would struggle to explain even the basics of the industry ecosystem given a four-hour slot, a flip chart and some coloured pens.

Key players such as the IAB made early moves to establish the Transparency and Consent Framework, and the "TCF", as it is increasingly known, has continued to gain traction this year. But many other players take the position that consent as a basis for processing is simply unworkable, instead opting to rely on the legitimate interests basis. In truth, neither of these legal bases was developed with AdTech in mind.

Debate also continues to rage as to whether various entities in the ecosystem should be characterised as "mere" processors, or controllers in their own right. A discussion made more complex by the fact that a single entity can legitimately take on either role at any one time depending on the purpose for which the data is processed.

In the meantime, the industry waits with baited breath for the next step in the glacial progression of the ePrivacy Regulation through the EU legislatures. While uncertainty reigns, publishers are feeling their way in search of GDPR compliance with a proliferation of consent management platforms, tools and menus being offered to users with the aim of giving them more information, choice and control over how their data is used for targeted advertising.

Sensationalist claims that the GDPR will spell the "death" of the AdTech industry as a whole are overblown and unrealistic given the current strength (and indeed wealth) of the industry. However, the GDPR (together with the impending ePrivacy Regulation) will undoubtedly change the landscape as we know it.

8

Will you be my Representative?

At the end of last year, the EDPB Guidelines on the territorial scope of the GDPR also attempted to answer some questions about the role and, most crucially, potential liability, of "Representatives" appointed under Article 27 of the GDPR.

By way of reminder, in broad terms, the GDPR (similar to the '95 Directive) obliges non-EU controllers and processors that process the data of data subjects in the EU to designate a representative in the EU. So far, it appears to be the least complied with obligation of the GDPR, with plenty of organisations ignoring it the same way they did under the Directive (presumably working on the basis that, with no representative, at least it's harder for the DPAs to take action against them for non-compliance…)

With Brexit on the horizon, however, this obligation has become more pertinent: not only will UK organisations operating in the EU need an EU representative but also – thanks to the UK's wholesale adoption of GDPR – EU organisations will now have to appoint a representative in the UK. Basically, everyone needs a representative everywhere. However, questions still remain over what role the representative should play in practice and, for those looking to appoint one, who is willing to take the role on?

So, what do we know? Well the Guidelines tell us that the representative role could be carried out by law firms, consultancies and other private companies in the EU. But it remains to be seen how many providers are actually ready and willing to carry out this role. The Guidelines also tell us that enforcement action can be initiated against a representative in the same way as against controllers or processors, meaning that there is the possibility for representatives to receive administrative fines and penalties, and to be held liable for the actions of the controllers or processors they represent.

However, there's still no clarity on the precise role the representative is expected to play. Is a representative a mere "letter box" for correspondence and enquiries between data subjects or regulators and the organisation? Or, does the fact that the representative is jointly responsible for the Article 30 record of processing and could be held liable for a substantive breach of GDPR, suggest that it is expected to have an in-depth understanding of its clients' processing operations, and perhaps even be involved in decision-making about the processing? Certainly, as a representative who could be held liable for their behaviour, you'd want to understand the compliance status of your client. (And get insurance maybe, assuming you can…?)

9 Regulating AI – easier said than done...

Public concerns are growing that cold and callous robots will soon displace fair and friendly humans in making decisions that will change our lives. Before we know it, they will be running the planet. In the best traditions of dystopian science fiction, we will have no idea what is going on, and we will be powerless to protect ourselves.

In fact, so-called 'AI' today is not Terminator-style 'General' or 'Strong' AI. Rather, it's about specific applications of machine learning ('Narrow AI'). While falling far short of the media hype, the impacts of narrow AI decisions can already be significant, for example if a machine makes an inscrutable decision about your employability or creditworthiness, or maybe gives you a rubbish score in a dating app.

GDPR was meant to calm everyone down by providing three main safeguards. The first is a restriction on the circumstances in which fully-automated decision-making processes can be deployed. The second is a requirement that people be given information about how such systems work. Finally, individuals have a right to demand that a human review an automated decision that has legal effects or similarly significantly affects them. So, it's good to know that has all been sorted out! The only problem is that the humans can't agree on how the rules are supposed to work. Ironic or what?

GDPR's Article 22, when read alongside Recital 71, doesn't cut it as a transparent and bug-free algorithm. The right not to be subject to an automated decision comes at the end of a list of rights that data subjects can exercise if they choose to do so, such as getting access to data, requesting correction or erasure of data, etc. Many people, however, are reading Article 22 as a general prohibition on automated decision-making that is subject to certain exceptions. Recital 71 doesn't clear up the issue, though the statement that "Such measures should not concern a child" may imply that the general ban shouldn't apply to decisions about adults.

What about the obligation (in Articles 13 and 14) to provide "meaningful information about the logic involved, as well as the significance and envisaged consequences of" automated decision-making? Some interpret this as a requirement to open the 'black box' and describe exactly how a decision was or will be reached. That makes little sense, not least because it may be impossible. Others claim it is about the 'explainability' of a decision and suggest that 'counterfactuals' may be the way to go. Again, that's not always going to be appropriate. If you were a bank, would you want to tell people exactly what buttons to push to get a (cheap) loan?

As for having a 'human in the loop', be careful what you wish for. Humans don't exactly have a great track record when it comes to making objective, fair, consistent, explainable, decisions. Indeed, most of the concerns about automated decisions concern the embedding of human bias in a machine learning process. How long will it be before the GDPR rule should be reversed? Why shouldn't we have a right to appeal to a robot against a decision made by an illogical or capricious human?

10 Has GDPR Worked?

Yes and no. Yes because it has raised the profile of data protection as a crucial corporate risk. It has prompted companies to invest, sometimes millions, in comprehensive compliance programmes, including modifying their IT systems, updating their customer and supplier contracts, coupled with an increased focus on cyber security. With storage being relatively cheap and the effort involved in 'weeding out' personal data being both time-consuming and expensive, historically, companies haven't been good at deleting or anonymising data once they're finished with it. GDPR has gone some way to improving this, forcing companies to grapple with data minimisation and data retention, often for the first time.

And nor should the other side of the coin be overlooked. Data subjects are now more aware of their legal rights – access, opt-outs, portability and erasure – than ever before. Another measure of success might be the extent to which we are seeing 'GDPR-like' laws being passed in other jurisdictions, not least in California, the home of many of the technology giants.

And why has it worked? It's hard to avoid the conclusion that for all the hype and scaremongering about maximum fines of 4% of global turnover, these new enforcement powers have focused many companies' minds. Whether turnover-based fines become common remains to be seen, but for the time being, the possibility of them seems to be enough.

But no, the GDPR hasn't worked on other levels. Back in 2010, when the idea of data protection reform was being discussed, one of the primary motivations was the need to have a law that was responsive to the challenges of new technologies, most of which were developed long after the data protection laws then in place. Technologies such as cloud computing, mobile apps, Internet of Things and artificial intelligence challenged the existing data protection laws. And so it was to be hoped that GDPR would regulate technology in an intelligent, relevant way. And yet, in so many areas it doesn't do so. The prohibition on automated decision-making clashes with many implementations of artificial intelligence. The requirement to have a 'processing basis' (consent, legitimate interests, etc.) seems to deny the ubiquity of data processing in modern, digital life. And requiring complex eco-systems, such as AdTech, cloud and the Internet of Things to address international data transfers is unrealistic, bordering on quaint.

But we'd like to end our review on a positive note. Let's not forget that we're all data subjects too. Regardless of the small print and teething problems, there's no denying that the GDPR has strengthened our privacy rights and the protection given to our personal data.

So Happy Birthday, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*

The **2018/19 Data Protection Top 10** was brought to you by the Bristows data protection team

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

Mark Watts
Partner
mark.watts@bristows.com

Robert Bond
Partner
robert.bond@bristows.com

Marc Dautlich
Partner
marc.dautlich@bristows.com

Christopher Millard
Senior Counsel
christopher.millard@bristows.com

Mac Macmillan
Of Counsel
mac.macmillan@bristows.com

Rebecca Anderson
Senior Associate
rebecca.anderson@bristows.com

Hannah Crowther
Senior Associate
hannah.crowther@bristows.com

Jamie Drucker
Senior Associate
jamie.drucker@bristows.com

Faye Harrison
Senior Associate
faye.harrison@bristows.com

Toby Headdon
Senior Associate
toby.headdon@bristows.com

Fiona Campbell
Associate
fiona.campbell@bristows.com

Michael Edgar
Associate
michael.edgar@bristows.com

Katy Gibson
Associate
katy.gibson@bristows.com

Charlie Hawes
Associate
charlie.hawes@bristows.com

Rosalie Hayes
Associate
rosalie.hayes@bristows.com

Emma Macalister Hall
Associate
emma.macalisterhall@bristows.com

Erik Müürsepp
Associate
erik.muursepp@bristows.com

Rob Powell
Associate
rob.powell@bristows.com

Janine Regan
Associate
janine.regan@bristows.com

Jamie Witton
Associate
jamie.witton@bristows.com

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

2019
33RD YEAR

The trusted source of privacy news, analysis and advice

Dedication to excellence in our field, maintaining regular contact with privacy regulators, and a network of specialists and resources worldwide help *Privacy Laws & Business* maintain its leading position.

REPORTS • CONFERENCES • CONSULTING • TRAINING • COMPLIANCE AUDITS
RECRUITMENT • PRIVACY OFFICERS NETWORK • ROUNDTABLES • RESEARCH

Privacy Laws & Business, 2nd Floor, Monument House, 215 Marsh Road, Pinner, Middlesex HA5 5NE, UK
Information: info@privacylaws.com Tel: +44 (0)20 8868 9200 **www.privacylaws.com**

International Report

Articles in recent issues include:

- Spain adopts GDPR implementing law
- How Ireland's DP Commission will exercise its powers
- Japan and Korea: Different paths to EU adequacy
- Cathay's data breach catastrophe goes beyond Hong Kong
- Finland's new Data Protection Act enters into force on 1 January
- US CLOUD Act creates global data access framework
- Brazil enacts Data Privacy Law
- California passes strictest data privacy law in the US
- Big Data, purpose use limitation and ethics under the GDPR
- Poland's new data protection law now in force

United Kingdom Report

Articles in recent issues include:

- Preparing for Brexit – EU to UK data export solutions needed
- How companies are adapting to the UK's DP Act 2018
- Employee Data Subject Access Requests and proportionality
- DPOs: Internal or external – the benefits and drawbacks
- Hitachi Consulting achieves BS DP certification 10012: 2017
- Jersey to stay in the European mainstream
- ICO promotes using certification and codes of conduct
- Cambridge Analytica whistleblower explains micro-targeting
- Beware of GDPR no-win no-fee compensation claims
- Aviva sees GDPR as leading to a new privacy culture

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.

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 a *PL&B* special report on data privacy laws worldwide published in 2019 and every two years.

Subscribe at privacylaws.com/subscribe

32ND YEAR

PL&B 32nd Annual International Conference

GDPR's influence ripples around the world

1-3 July 2019, St John's College, Cambridge, UK

privacylaws.com/annualconference

#PLBAC

Designed and Produced by ProCreative, Tel: 0800 228 9846

REPORT2PP 1.0 02/19

Successful businesses see things differently.

We are Bristows, the world's specialist law firm for clients that innovate.

We help clients grow in life sciences, technology and other dynamic sectors. Clients on the edge of tomorrow; those creating new technologies and ideas, and those embracing them. We provide advice on all their legal matters and we are proud to be different.

We are a European headquartered hub for litigation, transactions and advice throughout the world and have remained fiercely independent since we first began in 1837. This means we are free to partner with the best people in any jurisdiction for each client need, or work with your existing relationships. We don't work to billing targets.

This ensures you get the right combination of experts working as one, who take the time to share their different perspectives and find the right answer, no matter how difficult or novel the question is. It's a rare approach that defines the quality of our advice. And because we like to recruit inquisitive minds, many with science and technology backgrounds, we live and breathe your business, can talk the same language and have a keen eye on the future. We enjoy getting to the heart of the matter with advice that is simple to understand and easy to use.

Like any business we have evolved with time, but our focus and spirit have remained as resolute as the quality of our advice and as inimitable as the experience we deliver.

We are Bristows, seeing things differently for those shaping tomorrow.

Bristows LLP
100 Victoria Embankment
London EC4Y 0DH

T +44 20 7400 8000

Bristows Brussels
Avenue des Arts 56
1000 Bruxelles

T +32 2 801 1391

bristows.com

Bristows