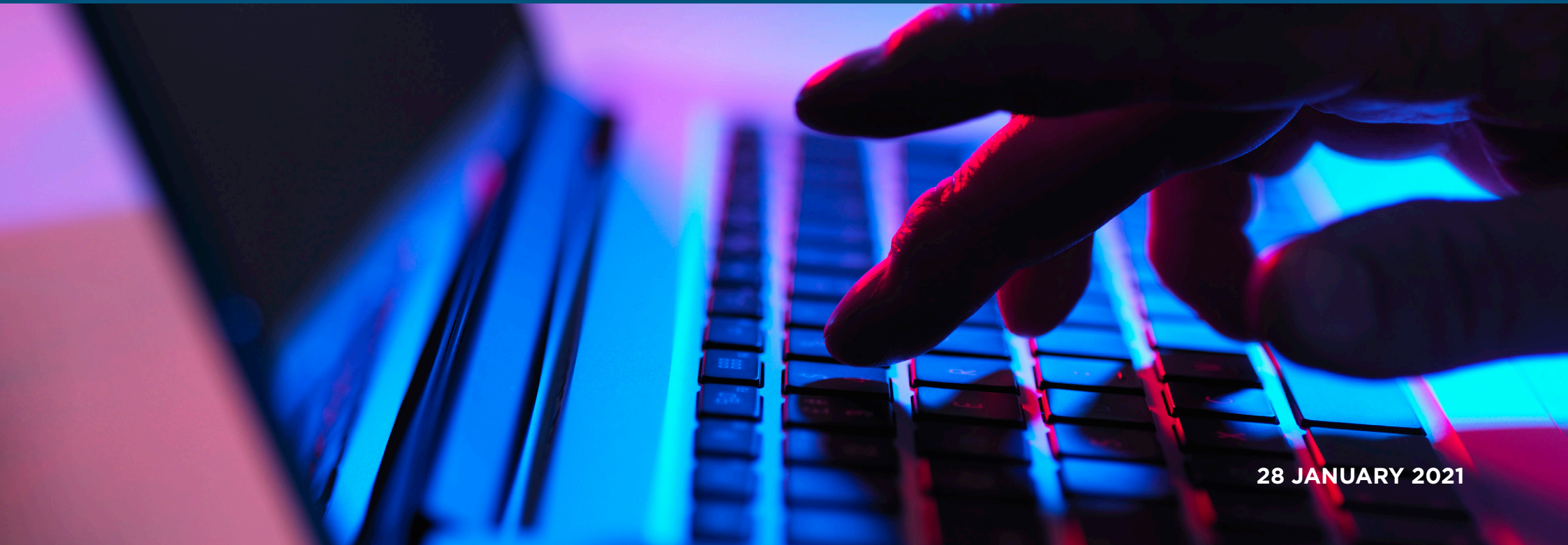




HERBERT
SMITH
FREEHILLS

HAPPY INTERNATIONAL DATA PRIVACY DAY

OUR PREDICTIONS FOR 2021



28 JANUARY 2021

Happy International Data Privacy Day: Our predictions for 2021

Happy International Data Privacy Day! And what better day than today, to explore what 2021 is likely to have in store for data and privacy? Almost three years after the EU General Data Protection Regulation (GDPR) came into force, and now 28 days since the UK GDPR replaced it in the UK following Brexit, data and privacy issues remain firmly in the spotlight for many organisations. And there are no signs that the rate of regulatory development is going to slow any time soon.

In this briefing, we set out our predictions for data protection and privacy developments in the year to come.



Adequacy decision for the UK

While data transfers from the EU to the UK may continue for the next four-to-six months with thanks to the last-hour EU-UK Brexit deal (further details available [here](#)), it is not clear what the implications of this interim data transfer window could be for the ongoing adequacy assessment being undertaken by the European Commission. Although some may be cautiously optimistic that the European Commission simply needs more time to dot its 'i's and cross its 't's with respect to adequacy, the relatively long shopping list of actions that the UK is prevented from taking in the field of data protection in order to keep this data transfer window open hints at a nervousness within the European Commission that the UK may move away from the principles of the GDPR in the future, something that could prevent an adequacy decision being granted in its favour. Coupled with the recent decisions of the ECJ in the Schrems II case (reported [here](#)) and the Privacy International case (reported [here](#)), it remains difficult to predict which way the adequacy decision is going to go. Either way, 2021 will be the year when we know whether or not the UK will be granted adequacy. And if granted, let us hope that it is not the year of a Schrems III-style challenge of any such decision!



Continued fallout from Schrems II

Following months of uncertainty after the July 2020 Schrems II judgment, the European Data Protection Board (EDPB) published its draft guidance and recommendations in November 2020 (reported [here](#)). Although any form of guidance was welcomed, the practical consequences of the EDPB's draft guidance remain a challenge for many organisations. The consultation period for the draft guidance closed in December 2020 and 2021 will hopefully see publication of the finalised guidance. We wait to see whether or not such guidance will offer organisations a more practical solution to the current international data transfer challenge.



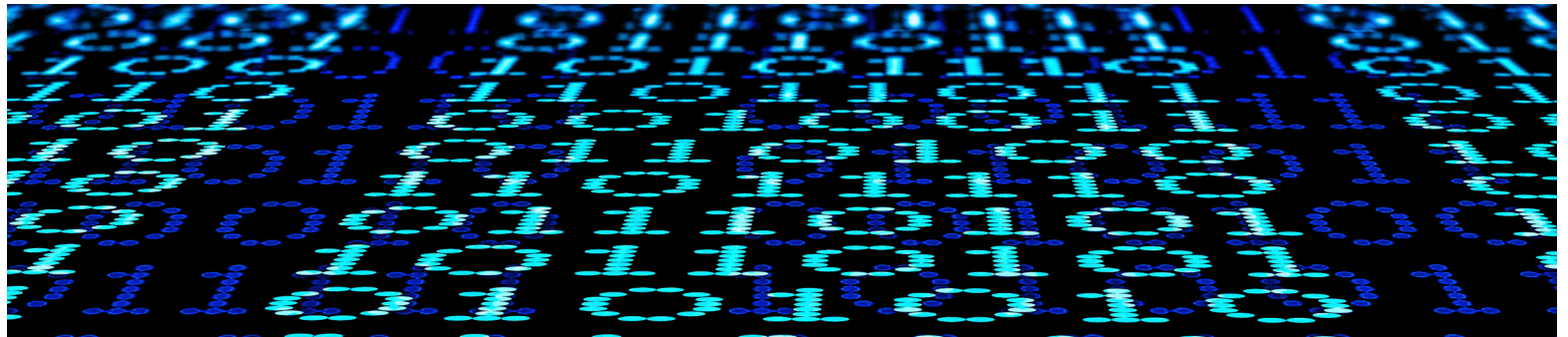
Data localisation on the rise?

Perhaps as a consequence of the fallout from Schrems II, it is possible that 2021 could see an increasing trend towards data localisation and regionalisation practices. Organisations wishing to avoid the time, effort and cost of due diligence on transfers or implementing supplementary measures, as well as those unable to navigate the, at times, impractical guidance from authorities, may well self-select to keep data in country/region rather than navigate the regulatory challenges now associated with international data transfers. It will therefore be interesting to watch the impact on global data transfers as a whole in 2021.



Transfers to the US – Safe Harbor 3.0?

Shortly after the Schrems II judgment, the US Department of Commerce and the European Commission initiated discussions to evaluate the potential for an enhanced EU-US Privacy Shield framework to comply with the ruling. However, even if this is developed over the course of 2021, without root and branch reform of US surveillance law, it remains unclear how any such framework would avoid the fate of its predecessors the Privacy Shield and US Safe Harbor. Perhaps a separate (and additional) question is whether 2021 could also see the UK forge its own path with the US to ensure UK-US transfers are enabled in accordance with the newly implemented UK GDPR?



Happy International Data Privacy Day:

Our predictions for 2021



New European Commission Standard Contractual Clauses

Continuing with the theme of international data transfers, 2021 is likely to see finalisation of the European Commission's new Standard Contractual Clauses which could be used by organisations to satisfy the data transfer restrictions set out in the GDPR (and currently the UK GDPR). The draft clauses were published by the European Commission in November 2020 (reported [here](#)) and the consultation on the clauses closed in December 2020. It is expected that a finalised version of the clauses will be published in 2021, with then a one year grace period for implementation.

As at the time of writing, the draft clauses would need to be put in place for existing as well as future data transfers, meaning that (yet another) mass repapering effort is likely to be required.



Article 28 Clauses – the new norm?

Shortly after, and perhaps in the shadow of, the European Commission publishing its long-awaited draft new Standard Contractual Clauses as described above, the European Commission also published in November 2020 a draft set of stand-alone Article 28 clauses for use between controllers and processors in the EU (reported [here](#)). Once again, the consultation period with respect to these draft clauses closed in December 2020 and a finalised version of the clauses is expected in 2021.

Although use of any finalised version of the clauses is not mandated, these clauses may have a substantial impact on how controllers and processors subject to the GDPR engage with each other going forwards.

Certainly the clauses leave room for discussion, in some areas more than others, but it may be that the European Commission's seal of approval for these clauses will render any attempted negotiation a non-starter.



Data continues to be a global issue

Moving away from Europe, the global trend of jurisdictions introducing or seeking to introduce more robust data protection laws, often similar to the GDPR, is also likely to continue in 2021.

China's draft Personal Information Protection Law was unveiled late in 2020; Australia is set to reform its Privacy Act of 1988; and New York and other US states also have proposed privacy legislation in the pipeline for 2021.

This may even be the year when the US puts in place a federal data protection law. Looking beyond 2021, a recent Gartner report (available [here](#)) suggests that, by 2023, 65% of the world's population will have its personal data covered under modern privacy regulations. Whatever 2021 brings, it is clear that global organisations will increasingly have to consider how to comply with multiple privacy standards.



The UK path

Which brings us neatly on to the UK. Will 2021 see the UK turn to, or away from, Europe with respect to data protection law? In theory, the UK is now free to forge its own path. And even though ECJ judgments handed down prior to the end of 2020 will continue to have precedence, there is nonetheless now a limited ability for the Supreme Court and Court of Appeal in the UK to deviate from such case law, including potentially Schrems II, where it appears right.

However, in practice, the UK cannot simply disregard Europe; not least given that any deviation could put at risk both the immediate data transfer window agreed as part of the Brexit Deal, as well as any potential future finding of adequacy.

As a result, 2021 is likely to see the UK trying to navigate and find a balance between potential changes to data protection law that it would like to implement in order to foster innovation and technology in the UK, as against its commitments under the Brexit deal and strong desire to ensure that the UK is considered adequate for GDPR purposes, thus avoiding a significant administrative and practical challenge for UK businesses going forward.

Happy International Data Privacy Day:

Our predictions for 2021



Data ethics

Data ethics was on our list for 2020 as we highlighted how organisations are coming under increased pressure, not just from consumers who are now demanding greater transparency around how their data is collected, used and handled, but also other stakeholders such as government, regulators, industry bodies and shareholders. This is only set to continue in 2021 as public awareness of data privacy and protection has grown due to Covid-19 and the role data has played in the pandemic.

The discussion continues to move from “what can we do” to “what should we do” with data in 2021, as organisations continue to incorporate ‘ethical practices’ into data strategies and promote transparency, to leverage consumer trust and drive long-term profitability.

In parallel, in 2021, we are set to see regulators continue to grapple with promoting the uptake of emerging technologies, whilst also addressing the unique challenges and risks arising from their use, including in respect of fundamental rights.



Privacy in the wake of Covid-19

Covid-19 will continue to cast a shadow in many ways over 2021, including with respect to data protection. The pandemic is likely to act as a catalyst for increased data sharing in 2021, as individuals become more willing to hand over their data for the ‘greater good’ and/or in exchange for simple freedoms – or, more concerning, because they are left with no choice. With reports that organisations are offering incentives to employees to have the vaccination, others looking to implement a “no jab, no job” policy or regular testing for employees, and ‘vaccination passports’ potentially being required to be able to board a flight, 2021 will likely see private organisations pushing the agenda and bring with it a raft of data protection and other legal implications.



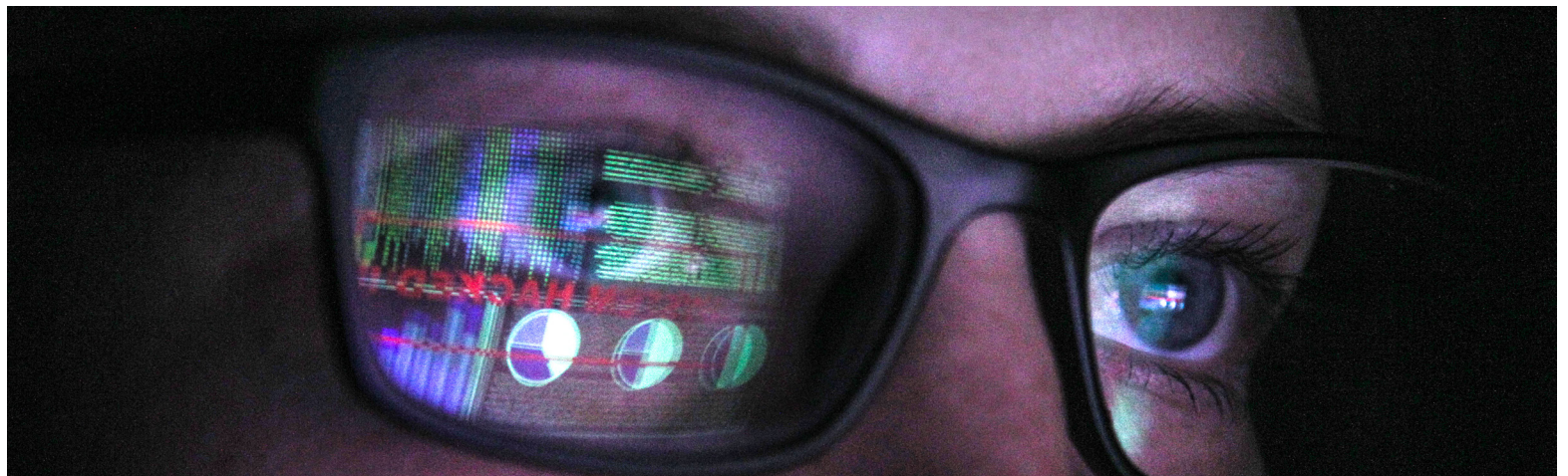
Data class actions

Following its 2018 data breach and the vastly reduced fine agreed with the ICO in 2020 (reported [here](#)), British Airways is now reportedly facing the largest group claim over a data breach in UK legal history, with reports that this could amount to at least £800 million if every affected individual came forward to “opt-in”. This class action will set the tone for those to come – if it does make it to court, although it has been reported that BA are looking to settle despite continuing to deny liability. In 2021 we are also expecting to see the long-awaited Supreme Court decision in the US-style “opt-out” representative action in the case of Lloyd v Google – which could significantly increase exposure for organisations following a data breach or other breach of the UK GDPR.



Lessons learnt being put into practice

2021 is also likely to see organisations putting into action the lessons learnt from GDPR enforcement actions, including the ICO enforcement action against BA, Marriott and Ticketmaster last year in connection with their respective breaches. One of the top takeaways was that cyber security must be prioritised and organisations must keep pace with emerging industry expectations, with arrangements with third parties needing to be carefully monitored as use of third parties does not diminish responsibility. However, statistics show that it is not just data breaches that organisations need to be aware of. Significant enforcement action in 2020 with respect to, for example, employee data in the H&M enforcement, has highlighted that it is not only consumer data that needs to be protected in 2021.



Happy International Data Privacy Day:

Our predictions for 2021



The role of the ICO, lead supervisory authority no more

2021 will see the start of the post-Brexit world where the ICO will no longer act as a lead supervisory authority under the EU GDPR.

But does this mean that 2021 will start to see pan-European organisations “forum shop” when selecting a main establishment in another EU jurisdiction where practical to do so?

What does this mean for ongoing enforcement cases for breaches under the EU GDPR where the ICO had been designated the lead supervisory authority? Can organisations assume that other EU supervisory authorities will recognise decisions made by the ICO? In 2021, it is likely that organisations and regulators will need to start to work through these post-Brexit questions.



ePrivacy

The update to the European legislation which regulates cookies and electronic marketing continues to be plagued by delays and disagreements, although an updated draft was published by the Council of the European Union in early 2021 after Portugal took over the presidency of the Council.

It is too early to tell whether this draft will secure the support of the other Members States, although the precedents to date are not favourable.

Even if 2021 is the year that ePrivacy is finally agreed in the European Union, considerations will then move to the UK's own approach to ePrivacy in a post-Brexit world.



Resumed spotlight on adtech

Now that the GDPR has started to become real for the adtech sector, attention also turns to complementary legislation that will continue to evolve in the year ahead.

The long awaited Digital Services Act and Digital Markets Act mark a new era for online regulation within Europe.

As they continue to progress through the European Parliamentary stages, we will see the new proposed transparency rules on online advertising play out front and centre for all online platforms, with much criticism levelled at target advertising in particular and high stakes for non-compliance.

Closer to home, the start of 2021 has already seen the ICO resume its investigation into real time bidding and the adtech industry (paused last year in the wake of Covid-19) and will continue with a series of audits focusing on digital market platforms to understand the lay of the land. With the ICO issuing a call to action for all adtech organisations to assess how they use personal data “as a matter of urgency”, will 2021 be the year in which we see meaningful enforcement action from the ICO in this area?

Authors



Miriam Everett
Partner
T +44 20 7466 2378
miriam.everett@hsf.com



Claire Wiseman
Professional Support Lawyer
T +44 20 7466 2267
claire.wiseman@hsf.com



Chloe Kite
Associate
+44 20 7466 2540
chloe.kite@hsf.com