

UPDATES

Governance of Data Innovation: Risks and Rewards for Business – Key Takeaways from our Discussion with the UK Information Commissioner’s Office

October 21, 2021

On September 21, 2021, Sidley partners Alan Raul and William Long engaged in a fireside chat with Elizabeth Denham and Claudia Berg of the United Kingdom (UK) Information Commissioner’s Office (ICO). Elizabeth Denham is due to end her five-year tenure as UK Information Commissioner on October 31, 2021. Claudia Berg is the ICO’s General Counsel. The webinar entitled “Governance of Data Innovation: Risks and Rewards for Business” touched on the crucial issues in data protection and cyberlaw including the future of international data transfers, emerging technologies, and Brexit. Please see below our “10 Key Takeaways” from this fascinating and timely discussion.

1. Objectives and Mandate of Global Forces in Data Protection — A Convergence A key point of discussion was the recent convergence in objectives and mandate among global forces in data protection. Both the June 2021 G7 held at Carbis Bay, UK, and the 2019 G20 held in Tokyo had the same theme: “to allow a free flow of data with trust.” Worldwide, regulators are also converging around a need for data protection legislation, as evidenced by China’s recent passing of its own data law: the Personal Information Protection Law (PIPL) (due to come into force on November 1). The discussion on convergence also highlighted the potential value in more international cooperation. The ICO believes that its current approach to data regulation, on a nation-by-nation basis, can only take data protection laws so far. To unlock the potential of data while maintaining public trust in how it is used requires a reimagining of data laws and the forging of an international solution — a form of data Bretton Woods, whereby we rethink data protection in the way that Bretton Woods rethought global financial systems toward the end of World War II.

Convergence also extends to relationships between regulators within the UK. For example, the UK’s competition law authority (CMA), the ICO, and Ofcom (the UK’s communications regulator) have together formed a Digital Regulation Cooperation Forum to support regulatory coordination in areas of mutual relevance. This convergence of regulatory efforts seems to have gone from strength to strength: Parties from all three organizations are regularly seconded to one another, and the ICO and CMA have published a joint statement on compliance.

2. New Proposed Reforms: There was also debate on potential future developments in UK data

protection law. For instance, on September 10, 2021, the UK government released its consultation entitled “Data: a New Direction” outlining its proposed reforms to the UK data protection regime. Particularly, the government’s paper cites an ultimate aim to create a more “pro-growth and pro-innovation data regime.” This position can be seen in the paper’s proposals to remove the current accountability framework in UK law and replace it with so-called “privacy management programmes” as well as the recommendation that the standard for reporting data breaches be lowered such that organizations need not report a breach that presents a “non-material” risk to data rights. However, the ICO underlined that the UK would be maintaining “high standards” of data protection.

3. International Transfers and the EU and UK’s Relationship: There was a lively discussion around some global trends toward localizing data as opposed to facilitating the free movement of data. One key issue discussed was that of Brexit and whether the European Union’s (EU) adequacy decision handed down to the UK will continue. This adequacy decision, in essence, allows for free data flow between the UK and EU due to a recognition of each other’s data protection regimes as “adequate.” The reasons behind this adequacy decision were discussed at some length, with the ICO suggesting that the UK’s robust checks and balances to the UK intelligence services’ potential access to EU citizen data was behind the EU decision to grant the UK an adequacy decision. Some confidence was expressed that the EU’s adequacy decision toward the UK will hold, given that the UK and EU have virtually the same laws, the UK has a strong data protection regulator in the ICO, and there is judicial oversight of UK intelligence services’ collection of data.

4. The “Special Relationship” — The US and UK Relationship Post-Brexit: Recent events have suggested a renewed enthusiasm for the “special relationship” between the UK and U.S. post-Brexit. One key point discussed was whether the UK may grant adequacy status to the U.S. for international transfers. The UK government’s recent paper certainly suggests an intention to add further countries to the list of those currently considered adequate by the UK.

The discussion on international transfers also sparked dialog on standard contractual clauses (SCCs) and their future. In June 2021, the European Commission published new SCCs following the *Schrems II* case. However, post-Brexit, the UK ICO has decided not to adopt the new EU SCCs and instead has drafted its own set of new UK standard contractual clauses (referred to as an international data transfer agreement or IDTA). The ICO is consulting on the draft IDTA and on questions related to its application of the UK GDPR to international data transfers.

5. Reporting Obligations and Cybersecurity: Cybersecurity and data breach reporting obligations remain a key issue for the ICO with a particular concern for new data-driven forms of criminality. The ICO is looking to focus resources on more serious cybersecurity attacks and ransomware rather than dealing with more minor accidental data breaches. Having said this, the ICO recognizes that the impact of a simple data breach can be serious, for example with the recent email that mistakenly revealed Afghan interpreters’ contact details, which potentially threatened their safety; it is scenarios like these that make drawing the line with reporting obligations difficult.

6. Emerging Technologies: One of the key challenges for the ICO is regulating emerging technologies such as artificial intelligence, machine learning, and facial recognition technology. The ICO recognizes a need to support innovation through digital development and have produced important practical tools to aid this process. For example, a recent ICO paper discusses the use of live facial recognition technology by law enforcement in public places, while another looks at the use of emerging technologies in the

commercial sector. Both papers show a commitment to providing guidance on *how* to use emerging technology instead of barring it. This approach ties in with the UK government's recent publication of its national artificial intelligence (AI) strategy, which further emphasizes unlocking the use of AI as opposed to over-regulating it.

7. Testing Technologies for Compliance and Governance: There was a discussion about the ICO's spirit of helping businesses use technology as opposed to entrapping them with regulatory obligations. This is shown in the success of the "Sandbox" scheme, whereby the ICO tests (and if needed remedies) apps that push the boundaries of data protection laws *before* they launch. The ICO emphasised the success of the scheme and how much businesses trust it: This may be due to the ICO's promise not to take enforcement action against those who use the Sandbox.

8. Data and Politics: In recent years there has been growing public concern regarding data use and its nexus with politics, and so there was some discussion on where the line is between legitimate persuasion and socially damaging manipulation of data. The key factor for the ICO is "transparency" — that people must understand who pays for political advertisements and why they are receiving them. If data is used "surreptitiously," it is probably not legitimate.

9. Tradeoffs and the ICO's Mandate: The ICO holds a unique position in having a mandate not only to regulate data but to be mindful of other factors including "economic growth." Thus, discussion focused on how the ICO's mandate may be affected by the recent UK government consultation discussed above. The ICO's view was that the proposals amount to an extension of its mandate, as consideration would have to be given to further factors such as public safety when considering data compliance. The ICO further believes that there is always a balance between data privacy and other factors, as no country considers privacy to be an absolute right. The ICO is therefore accepting of the government's proposal to widen its mandate but added that its lens would continue to be checking high standards of data protection and keeping people at the center of how data is used and regulated.

10. The ICO Mission and Closing Remarks from Elizabeth Denham on Her Tenure: The discussion with Elizabeth Denham was well timed given it is her last month in office. The Commissioner highlighted the excellent team that has been built at the ICO and her desire for the ICO to continue focusing on real issues that affect the public at large, including children and data, cybersecurity, and artificial intelligence. It will be absorbing to see how these issues are viewed and prioritized under the leadership of incoming Commissioner John Edwards.

To access the recording from our recent discussion with the ICO, click [here](#).

Thank you to Sidley Law Clerk Subhalakshmi Kumar for her significant contribution to this Update.

CONTACTS

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work, or

William RM Long, Partner

+44 20 7360 2061, wlong@sidley.com

Attorney Advertising—Sidley Austin LLP is a global law firm. Our addresses and contact information can be found at www.sidley.com/en/locations/offices.

Sidley provides this information as a service to clients and other friends for educational purposes only. It should not be construed or relied on as legal advice or to create a lawyer-client relationship. Readers should not act upon this information without seeking advice from professional advisers. Sidley and Sidley Austin refer to Sidley Austin LLP and affiliated partnerships as explained at www.sidley.com/disclaimer.

© Sidley Austin LLP