

REGULATORY INTELLIGENCE

Data protection horizon scan for financial services in 2022

Published 20-Jan-2022 by

William Long, Francesca Blythe and Eleanor Dodding, Sidley

As a new year begins and the [EU General Data Protection Regulation](#) (GDPR) moves into its fourth year, developments in the privacy sphere both in Europe and beyond show no sign of slowing down. The last year has seen several significant developments set in motion across Europe and internationally that will provide for a busy year ahead from a data protection perspective for financial services firms, as discussed further below.

International transfers from the EU

Following the CJEU's [Schrems II case](#) back in July 2020, which invalidated the EU-U.S. Privacy Shield for international transfers and placed additional requirements on companies seeking to rely on standard contractual clauses (SCCs), the European Commission published a new (more onerous) set of SCCs (new EU SCCs) in June 2021.

Firms should now be using these new EU SCCs for all new contracts involving international transfers of personal data from/originating in the EU, and in 2022 will likely need to implement a process for updating existing contracts to include the new EU SCCs i.e., prior to the December 27, 2022 deadline.

The Schrems II case also imposed an obligation on companies to conduct transfer impact assessments (TIAs) and firms should continue to prepare and maintain their TIAs to map the relevant data flows and assess whether the third country offers "essential equivalence", particularly given an increased focus on this requirement by the European Data Protection Board (EDPB).

The EDPB has also published various new guidelines to assist firms with navigating these developments. Of particular interest for 2022 will be the final version of the guidelines on the "Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR".

The guidelines seek to provide clarity to the European Commission's Recital 7 of the new EU SCCs, including a helpful statement that transfers directly from individuals in the EEA to third countries will not be classed as a restricted transfer (e.g., when submitting personal data via a website hosted in the United States).

A new set of SCCs is also expected to be published by the European Commission in the first half of 2022 for companies based in third countries outside the EU which are still subject to the GDPR.

These developments, together with the UK data transfer developments (discussed below), means firms are far from having one set of harmonized (or finalized) contractual provisions to address multinational data transfers and will need to focus in 2022 on international data transfers and putting in place the new SCCs.

UK data protection post-Brexit

For firms based in the UK, close attention will be required to the continued development of the UK's approach to data protection post-Brexit. In 2021, the UK published a number of documents setting out its proposal for "a new direction" in data protection, including: its consultation on its "Data: A New Direction" reforms (consultation); the UK's approach to adequacy; and its own form of International Data Transfer Agreement (IDTA) and TIA. Particular points to note from these UK developments include:

The consultation sets the agenda for proposed reforms to the UK data protection regime post-Brexit, to help "drive growth, innovation and competition". The proposals include changes to the legitimate interest assessment process, amendments to the requirements around automated decision making in [Article 22 UK GDPR](#) (e.g., removal of the need for human review) as well as reworking rules with regards to cookies and direct marketing.

The consultation also looks at reform of the UK Information Commissioner's Office (ICO) to assist it in taking an active approach to its regulatory activities, allowing the ICO, for example, to increase its strategic outreach to sectors using data in innovative ways, including financial services.

The consultation confirms the UK's desire to carve its own path away from the EU GDPR. However, with the UK receiving an adequacy decision from the European Commission in 2021 based on the UK data protection regime, it remains to be seen to what extent the UK can deviate from the EU on data protection.

In addition, the UK government's mission statement setting out its approach to adequacy assessments sees the UK go beyond the EU's adequacy decisions and aim to prioritise "data adequacy partnerships" with new territories including Australia, Dubai International



THOMSON REUTERS™

© 2022 Thomson Reuters. No claim to original U.S. Government Works.

Finance Centre and the United States. Firms will look keenly to see whether the restrictions imposed on international transfers to certain key business hubs could be eased by the UK.

The UK did not adopt the new EU SCCs in June 2021 (see above). The UK has instead been consulting on its own form of IDTA and TIA, including a UK addendum to the new EU SCCs.

There are several distinctions between the UK IDTA and the new EU SCCs, for example, the IDTA is not modular and does not contain Article 28 UK GDPR processing provisions. Final versions of these documents were originally expected at the end of 2021 but it is understood that these will now be published in early 2022. Firms will be interested to see final versions of these key documents and how this documentation will sit alongside the new EU SCCs, given the EU and UK regimes apply in parallel to many firms.

e-Privacy Regulation

Having been in draft since 2017, last year saw a long-awaited agreement by the Council of the European Union on the EU e-Privacy Regulation proposal, intended to replace the existing [EU e-Privacy Directive 2002/58](#) and which protects the confidentiality of electronic communications (e.g., e-mail, SMS, voice-over-IP and other Over-The-Top services etc.).

The regulation will regulate key activities such as cookies, the sending of unsolicited direct marketing, and also AI and machine-to-machine communications and includes a number of key differences when compared with the existing legal framework, for example, a broader extra-territorial reach, including a requirement to appoint an EU representative, an expansion of scope to cover "over-the-top" services, and an attempt to simplify the rules relating to cookies (including a proposal to remove consent requirements for certain non-privacy intrusive cookies such as those measuring audience numbers), among others.

While it is expected the regulation will now not come into force until 2024 at the earliest, firms should continue to monitor these developments in 2022 and consider how the regulation may impact them.

Regulation of artificial intelligence

In 2021, the EC published its proposal on the EU Artificial Intelligence Regulation. The AI regulation proposal includes rules around placing on the market and the transparency obligations, and specific requirements for providers of "high risk" AI systems, adopting a risk-based approach to regulation.

The draft AI regulation provides for maximum fines which far exceed those in the EU/UK GDPR, namely 30 million euros or 6% of worldwide annual turnover (versus 20 million euros or 4% imposed by the EU GDPR).

Relatedly, the UK government has also published its own national AI strategy which, in line with its data protection regime proposals, sets out an agenda to build the most "pro-innovation regulatory environment in the world". Notably, there is some divergence from the EU GDPR, including (as mentioned above) consideration of whether to remove the restrictions on automated decision-making set out in Article 22 GDPR.

The UK's white paper on regulating AI is expected in early 2022 before draft legislation is formally presented to the UK parliament.

Cybersecurity

Cybersecurity and data breach reporting obligations are set to remain key issues for firms in 2022. At the end of 2021, the [Apache Log4j vulnerability](#), which allows for potential unauthenticated remote code execution by threat actors, affected a huge number of applications used by companies and highlighted the continued threats to cybersecurity faced by companies, including but not limited to firms, in general.

More generally, significant increases in ransomware attacks have been widely reported. In the light of these developments, there may be some changes on the horizon as to how regulators deal with security incidents, including personal data breaches. For example, the UK government has recognised the difficulties with overreporting in its consultation which considers the need to only report "material" breaches.

This may result in a distinction being drawn for firms in their incident response reporting procedures for UK and EU breaches respectively (alongside the existing differing requirements internationally).

Enforcement action

Alongside cybersecurity incidents, enforcement action by EU DPAs continued to increase throughout 2021, in both volume and the amount fined, a trend which the authors expect to continue this year. Enforcement was wide ranging, dealing with alleged breaches of transparency requirements, obtaining valid consent and personal data breaches, among other topics. Last year also saw some of the largest GDPR fines issued to date.

As well as highlighting that DPAs have teeth when it comes to enforcing compliance with monetary penalties, enforcement action has knock-on effects for highlighting continuing compliance requirements, demonstrating in particular the areas where DPAs are focusing their attention. Firms should continue to monitor enforcement action to ensure they remain up-to-date with regulatory recommendations and market practice.

Global privacy law developments



THOMSON REUTERS™

© 2022 Thomson Reuters. No claim to original U.S. Government Works.

Looking beyond the EU/UK, multinational firms will also need to consider a variety of privacy law developments in other jurisdictions which have recently come into force or are expected in the coming years, including in China (with the introduction of the Personal Information Protection Law on November 1, 2021), India's Data Protection Bill and in the United States (which has a number of state laws, including the Colorado Privacy Act and the California Privacy Rights Act coming into force in the next couple of years).

Firms should consider if these new laws will have an impact on them and take steps during 2022 to prepare for compliance, including considering whether a global privacy program should be developed to address these developments.

William Long, Francesca Blythe and Eleanor Dodding, [Sidley](#)

[Complaints Procedure](#)

Produced by Thomson Reuters Accelus Regulatory Intelligence

24-Jan-2022



THOMSON REUTERS™

© 2022 Thomson Reuters. No claim to original U.S. Government Works.