IRSG

INTERNATIONAL REGULATORY STRATEGY GROUP

RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA

The International Regulatory Strategy Group (IRSG) is a practitioner-led body comprising leading UK-based representatives from the financial and professional services industry. It is an advisory body both to the City of London Corporation, and to TheCityUK. The Data workstream includes representatives from financial services firms, trade associations, the legal profession and data providers.

We welcome the opportunity to contribute the following comments, following the European Data Protection Board (EDPB) publication of supplementary guidance on how organisations should approach international data transfers of GDPR-covered personal data. The IRSG will also respond to European Commission's call for feedback on their draft set of new standard contractual clauses (SCC), and previously contributed to the European Commission's review of SCC in October 2019. In responding, we would like to highlight the following concerns from our Members:

1. ***Perceived lack of risk-based approach***

There is a perceived lack of a 'risk based' approach in the requirements set out in the recommendations. As the 'risk-based approach' was a large part of the GDPR accountability model, it is unclear why it is not part of the recommendations in question. In addition, the case studies appear to consider the same risk for all personal data sent outside the EU. For example, Use Case 7, whether in-scope data is intra-group access to an internal employee data (like a staff directory), or external access to other types of more sensitive personal data). Not only does this run contrary to a 'risk-based approach', it also contradicts risk-based assessments advised by EU regulators in other areas, for example, what constitutes a 'likely' and so regulator-notifiable, data protection risk in data breach assessments.

In addition, such a strict approach also risks countering Charter values, as the Charter of Fundamental Rights includes a necessity and proportionality test to frame limitations to the rights it protects. They also suggest the need for a different approach in assessing of EU businesses handling personal data, rather than other businesses – regardless of the practical risk or likelihood of national security interest in the personal data in scope. The IRSG is concerned of a potential 'one rule for them, one rule for us' scenario, which the CJEU was keen to dispel in its data retention judgement on the 6 October 2020.

2. ***Difficulty in assessing the law in third countries***

The expectation that the data controller can seek advice from the importer on local laws and customs seems to be a conflict of interest with those of the importer who may tell the controller whatever they want to hear to win the work. This would be an issue especially in jurisdictions where importers do not have an EU presence within the enforcement scope of the EU. In addition, the measures do not appreciate of the lack of equivalent resources that companies will have in comparison with the Commission and the regulators. This includes lack of equivalent political resources and the influence; lack of internal specialist knowledge to opine on third country national security issues which are outside of business expertise or purview; the far more tight commercial timescales that will exist in practice to meet business goals, and to cover compliance of existing commercial set-ups.

The IRSG believes it should be for the national Data Protection Authorities to determine whether the local laws and customs of a third country create a GDPR obstacle to a transfer of data to that country. The suggestion that this responsibility will rest with the data controller will simply be unworkable and price many companies out of the international market.

3. Compliance with supplementary measures

These recommendations present more onerous obligations on controllers and processors, with no grace period to work to compliance. Understanding 'publication' is in final form – rather than on first publication on 11 November, then they will be applicable immediately following their publication. If publication means they are effective now, whilst open to consultation, this risks resource in complying with rules that could be subject to change, following assessment of received consultation responses.

Given that companies can have thousands of vendors as well as a complex web of data transfers with customers and within their corporate group, and given the complexities this topic presents, this will take time to complete. The IRSG would appreciate clarity on this matter, and would like to see a longer transition period provided, e.g. two years.

Some of these requirements are very detailed, for example the six requirements asked of encryption, and will require operational and technical assessment to assess the feasibility and alignment of these to current industry working practices. The IRSG argues that this level of detail is best left to business to assess, rather than be prescribed by regulators. Furthermore, some cloud providers may mandate companies today to share cryptographic keys, thereby placing companies who want to comply with these recommendations, with risk of breaching current contractual arrangements.

For any questions or clarifications please contact: IRSGsecretariat@cityoflondon.gov.uk.

ANNEX – IRSG DATA WORKSTREAM MEMBERSHIP

- Refinitiv
- ABI
- AFME
- AIMA
- Bank of America
- Barclays
- BNY Mellon
- CBI
- Citi
- Clifford Chance
- Credit Suisse
- DLA Piper
- Fidelity
- FLA
- Freshfields
- HSBC
- IA
- Invesco
- IBM
- JP Morgan
- Lloyds Banking Group
- London Stock Exchange Group
- Marsh Ltd
- Mastercard
- Morgan Stanley
- Nasdaq
- PIMFA
- Standard Chartered
- techUK
- UK Finance