

IRSG DATA WORKSTREAM RESPONSE TO CONSULTATION ON EUROPEAN STRATEGY FOR DATA

The International Regulatory Strategy Group (IRSG) Data workstream is pleased to respond to the European Commission's consultation on a European strategy for Data. We value the Commission's recognition of the importance of the global digital transition that is currently changing our societies and economies at unprecedented speed, and the position of data at the core of this transformation.

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

In particular light of the COVID-19 crisis, the IRSG Data workstream by means of this letter would like to set out some of its thinking on how data governance mechanisms and structures can best maximise the social and economic benefits of data usage in the EU. We recognise that a consultation is currently ongoing on how the financial services sector could best harness the data economy, however we feel that there are some broader topics to consider in response to this consultation. In particular, the IRSG Data workstream has identified the following issues as those to note:

1. The importance of remaining internationally connected in regards data access and sharing.

We support the development of common European data spaces, but a lot of work is needed to determine how these will operate and how they should be governed. The IRSG Data workstream believe that the most appropriate governance role for authorities is a high level one. This should involve establishing principles of access and playing a convening role to achieve interoperability between data spaces, alongside developing any necessary standards on how to access data. According to McKinsey, cross-border data flows now make a larger impact to global GDP than trade in goods¹. It is therefore vital to recognise the importance of the EU within the global landscape. As technology and data are increasingly borderless, it is essential that any EU framework takes into consideration the international dimension and interoperability with approaches taken in other countries. Specifically, there is a need to support data sharing across borders by better enabling the current mechanisms which do not reflect the realities of "data sharing" vs "data transfers", and that for big data, consent is unlikely to be a practical mechanism.

As way of example, the need to remain internationally connected is crucial in order to effectively identify, respond and fight financial crime and cybercrime. The fight against financial crime and cybercrime is a cross-jurisdictional issue and requires the processing – and specifically the sharing – of personal data across borders to be effective. This is something that the FATF has acknowledged in their recent report on COVID-19 and AML/CFT².

2. The need to be agile and flexible in the data approach to be able to respond to external threats, such as COVID-19.

¹ McKinsey Global Institute. (2016). *Digital globalization: The new era of global flow*.

² Financial Action Task Force. (2020). *COVID-19-related Money Laundering and Terrorist Financing*.

We agree with the European Commission's assertion that:

"Fragmentation between Member States is a major risk for the vision of a common European data space and for the further development of a genuine single market for data."³

Nevertheless, for data practitioners, there continues to be unhelpful national variations in interpretation of regulation between the Member States. One particular example is in relation to outsourcing and use of cloud. The European Banking Authority Guidelines on Outsourcing Arrangements⁴ have helped harmonise requirements across the EU but material differences remain between NCAs. This lack of clarity limits the ability for businesses to share data across the EU. With the actions that flow from this strategy, the EU should promote regulatory harmonisation and create common standards across jurisdictions, and seek to prevent conflicting supervisory practices.

The current COVID-19 crisis serves as evidence of this, with differing views on the ability to process special category data published from various data protection authorities. While the statement from the EDPB⁵ was both balanced and even-handed, some Member States have taken a more restrictive view whereas others have been pragmatic, for example by acknowledging that the GDPR does not hinder both public and private sector initiatives to respond to Covid-19. The creation of a common data space in line with the aims of this strategy will require the support of both regulators and legislators. However, the diverging views and lack of coordinated guidance in light of COVID-19 would suggest that there is still work required to remedy this.

3. The need to recognise the breadth of legitimate interests in terms of processing personal data.

The workstream also notes that the European strategy for data intends to:

"strengthen the governance mechanisms at EU level and in the Member States relevant for cross-sector data use and for data use in the common sectoral data spaces, involving both private and public players."⁶

The IRSG Data workstream are keen to stress that a lot of what is essential cannot be done by the public sector alone. COVID-19 has shown this in the context of a health crisis, however private organisations also have a role to play in helping government reach its policy aims. Nevertheless, it continues to be challenging for the private sector to apply some of the public interest grounds for processing under the GDPR. It is important that the diverse issues which arise depending on the nature of the data holder and data user, for example business-government, business-business or government-business, are all addressed.

We welcome the strategy's recognition that data from the private sector can also make a significant contribution as a public good. Again, COVID-19 has provided evidence that collaboration between

³ European Commission. (2020). *A European strategy for data*, p. 6.

⁴ European Banking Authority. (2019). *EBA Guidelines on outsourcing arrangements*.

⁵ European Data Protection Board. (2020). *Statement on the processing of personal data in the context of the COVID-19 outbreak*.

⁶ European Commission. (2020). *A European strategy for data*, p. 12.

private and public sector is critical. However, in this context the intersection between privacy and other regulatory requirements continues to lack clarity i.e. processing of special category data may be permissible under GDPR, but is restricted by Member State employment laws. It is our expectation that the public sector will rely more heavily on the private sector going forward, especially if recently published economic forecasts are correct, and the public sector will be under increased financial constraint in future. This increasingly integrated public/private relationship is both inevitable and positive, therefore it requires support from both regulators and legislators.

In the new digital economy, firms will leverage data to innovate and build and maintain digital trust. The winning financial institutions of the future will put data at their core in order to survive and thrive in the digital economy. Continued fragmentation between Member States creates uncertainty; however it also creates a situation where businesses are reluctant to innovate, reluctant to take risk, and where they are fearful to share information.

Innovation relies on the ability to be quick, agile and nimble, and we agree that Europe should offer an environment that supports data-driven innovation. However, the response and guidance issued by various data protection authorities in the context to COVID-19 was neither agile nor nimble, nor responsive to what business and government necessarily needed. This is an example of why it is so critical that the EU encourages a positive data environment where data is not only protected, as it is with the GDPR, but where innovation can also occur and be supported.

Contact address:

IRSGSecretariat@cityoflondon.gov.uk

IRSG DATA PROTECTION WORKSTREAM – MEMBERSHIP

ABI	Impax Asset Management
AFB	Invesco
AFME	JP Morgan
AIMA	Lloyds Banking Group
Bank of America Merrill Lynch	London Stock Exchange Group
BNY Mellon	Marsh UK & Ireland
CBI	Mastercard
Citigroup	Morgan Stanley
Clifford Chance	Nasdaq
Credit Suisse	Norinchukin Bank
Deloitte	PIMFA
DLA Piper	PwC
Fidelity	Refinitiv
FLA	Scottish Development International
Freshfields	techUK
HSBC	TheCityUK
IA	UBS
IBM	UK Finance