IRSG
INTERNATIONAL
REGULATORY
STRATEGY GROUP

European Data Protection Framework Proposals

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 Data Protection workstream has representatives from financial services firms, trade associations, the legal profession and data providers.

We recognise the need to update the existing Data Protection Directive, aiming to create a uniform data protection regime across the European Union. However, we are concerned about the Regulation proposals as currently drafted which we believe.

- would not deliver the discernible benefits intended for data subjects whilst placing significant additional burdens on organisations;
- could cause inconsistency and duplication among existing EU and international laws and regulations to which financial institutions are subject;
- could affect consumer protection measures to prevent or detect fraud or financial crime;
- could impact on the inward business investment into the EU.

Accountability

The Regulation aims for greater accountability of data processors and controllers. However, we are concerned that the current proposals would give little or no additional benefit to individuals whilst being over-prescriptive and increasing the burden on business. The existing Directive (95/46/EC) adopted a principles-based approach, but the proposals add rules which data controllers must follow in order to comply with the principles. Mostly, these rules do not take account of the nature and context of processing. For example, requiring organisations to justify the purposes and envisaged consequences of data processing, to the customer on request may not always be necessary since this is often clear to the customer - for instance a mortgage application.

There is confusion about the 'right to be forgotten' (RTBF) and its scope for both organisations and individuals. Telling consumers there is an RTBF is misleading as many forms of customer data held by, for example, finance companies and insurers must be held for specific periods by law. The right to be forgotten must be appropriately designed to ensure that:

- consumers are not misled about their rights to have data deleted;
- it cannot be exploited to remove data for fraudulent purposes;
- it does not interfere with contractual obligations between organisations and customers;
- it recognises the need for organisations to retain data for specific periods by law.

Proportionality

We recognise that the proposals mean some reduction in administrative procedures undertaken by firms. But, on balance the administrative burden on firms will increase with no discernible benefit to individuals. A one size fits all approach is neither reasonable nor sustainable for smaller organisations. Measures should be proportionate to the nature/size of the business and level of risk to privacy involved. The following examples illustrate our concerns:

- mandatory data privacy impact assessments (Article 33) are overly prescriptive, particularly the stipulation that data controllers "seek the views of data subjects or their representatives on the intended processing". Additionally, the circumstances where an impact assessment is required have not been clearly defined.

- explicit consent (Article 4(8)) – requiring this for each separate purpose would be time-consuming for the consumer and resource-intensive and costly for businesses. People will not read long notices / consents which will therefore fail in their intended purpose, adding only a barrier and cost to services.
- information to be provided to the data subject (Article 14) and the broad areas where fines can be applied (Article 79).

Uses of data

The proposed Regulation must not interfere with the ability of businesses to comply with regulatory and similar obligations. The financial services industry must comply with a broad range of legislative and regulatory measures on processing of personal data. The proposed Regulation does not fully recognise this (e.g. in relation to anti-money laundering, fraud, and IT security). These uses of data should be explicitly recognised in the drafting of the Regulation.

We are extremely concerned that proposals may impact on organisations' ability to process and / or share data to prevent and detect fraud and other financial crime. Fraud prevention and detection is an important form of consumer protection and the Regulation should explicitly recognise and support, not restrict efforts to combat fraud. Whilst we believe that Article 6 encompasses data sharing for fraud purposes for non-sensitive data,[1] it is not clear whether there is sufficient flexibility in the Regulation for sensitive data to be shared for these purposes. Of particular concern is the restriction in the use of criminal conviction data. Banks are required to maintain all types of data relating to fraud, anti-money laundering and anti-terrorist financing investigations. The use of criminal convictions data is also vital for insurance fraud detection. The proposed Regulation must recognise these activities as a legitimate basis for processing and permit storing data on criminal convictions.

International/extra territoriality

We are extremely concerned at the extra-territorial impact of these proposals, amounting to the imposition of EU rules on conduct undertaken in other jurisdictions. This could lead other jurisdictions to seek similar powers over data processing by their subsidiaries within the EU, and enhance the likelihood of incompatible regulatory requirements and conflicts of law. It could also harm the EU's ability to negotiate agreements on data processing and data transfer with third countries. We believe that this is likely to act as a disincentive to non-EU firms to provide services into the EU, as the proposals make personal data processing less attractive to them. This will ultimately result in reduced choice for consumers. As currently drafted the proposals would also apply to non-EU firms with solely non-EU based clients who wish to seek the services of an EU-based data processor.

We do not believe that the current proposals significantly improve on the existing use of Binding Corporate Rules (BCR) for International data transfers as the BCR now require EDPB approval, and the requirements continue to be overly restrictive. We believe that data exporters should remain responsible wherever processing takes place and have the tools necessary to assess risk and ensure compliance. A self-certification model for which controllers are accountable for compliance would be more workable and promote, rather than deter, data protection compliance.

Contact: Audrey Nelson, IRSG Secretariat

audrey.nelson@cityoflondon.gov.uk

[1] Article 6, Clause 1 (f) 'processing is necessary for the purposes of the legitimate interests pursued by the controller'