

## **IRSG High Level Position Paper on Global Data**

*The International Regulatory Strategy Group (IRSG) is a cross-sectoral 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 workstream has representatives from financial services firms, trade associations, the legal profession and data providers. Most members operate within extensive and mature regulatory frameworks, and are finding that the way in which the data legislation environment is evolving is inhibiting members' ability to process data as necessary to comply with that regulatory framework.*

The world continues to swiftly evolve, and we currently live in the digital information age. The unprecedented availability of information as a result of being in digital form is transforming how data is handled, what it is used for, and how it is protected.

Fundamentally, a balance needs to be achieved between the freedom of general data use and personal data protection. Too much of one or the other will have significant adverse effects on economic development and personal protections. The growth agenda needs to be supported and nurtured, and balanced data legislation is key to achieving this.

The members of the IRSG encourage a healthy debate of these issues, and recognise the importance of the use of data to develop economies, connect people and create opportunities for growth. It is equally important that personal data rights are respected, and that data is not misused. The right balance of incentives is required to encourage responsible data handling practices.

The proposed EU Data Protection Directive and Regulation are important in setting standards for data protection, but it is essential to consider broader realities of data such as mobile, cloud, internet etc. How the EU reacts to the realities of the digital age helps to set the international profile on these important issues, and changes which may appear to be small or incremental at the EU level may have significant impact or consequences, including unintended consequences, at the international level.

### **Opportunities of the Internet and Mobile technologies, and Globalisation**

- The Internet, Mobile technologies and the phenomenon of Globalisation facilitates the provision of goods and services in ways that were not contemplated a few decades ago, enabling new businesses to flourish on-line, opening opportunities for existing businesses of all sizes (down to micro-businesses) to reach new customers and evolve and grow, enabling participation in global supply chains, and opening new opportunities for competitive pricing.

- Data analytics create opportunities for growth, innovation and job creation through new and smarter ways of doing business and connecting people. Appropriate technical and organisational measures are integral to safeguarding data in a fast evolving environment, and one where customers continue to demand individualised on-line services and are increasingly technically savvy across all generations, as well as demonstrating increasing awareness and exercise of their privacy rights.
- Given these opportunities, it is inconsistent to encourage global investment and franchise expansion on the one hand, and to restrict data-flows, require localisation of data-processing and inhibit compliance with requirements of foreign jurisdictions, on the other.

### **Restrictions on Data Movement and Data Sharing**

- Data-movement and data-sharing practices are steadily evolving, and will continue to do so. The trend is towards increasingly global flows of data, as the basic stock-in-trade of global commerce. As a result, geographical restrictions are becoming obsolete, because they no longer reflect current concepts of data-movement and data-sharing or the realities of commercial data-use in the 21<sup>st</sup> century.
- While data protection and security are essential, restrictions on processing and sharing data stifle growth for all sizes of business, and ignore the realities of the cloud and Internet data flows. The reality is that the globally integrated economy runs on a global platform where geographic restrictions are increasingly outmoded.
- The need for access to data by Government and relevant authorities is recognised as important to safeguard society and to counter crime and terrorism. However, the imposition of data restrictions on large firms operating in multiple jurisdictions makes it difficult to achieve this objective. Restrictions on the movement of data introduce conflicting obligations for the private sector, and will impinge on its ability to help Government and relevant authorities to combat financial crime. In addition, new data collection, reporting and transparency obligations are introducing weighty compliance burdens. Rules on access to data for Government and relevant authorities, as well as reporting requirements, need to strike an appropriate balance between the potential conflicts inherent in a web of differing needs and obligations.
- Free flows of data are particularly important to guarantee the ability of global firms to carry out intra-company data transfers across businesses operating in multiple jurisdictions. This transfer of data can be important for a number of reasons, not least to support risk reporting and the detection of criminal activity. The efforts of firms to combat fraud should be supported,

particularly in the development data protection legislative framework, to permit the use, sharing and transfer of data to combat fraud and other criminal activity.

### **International Support for Digital Trade**

- A global solution focussed on mutual recognition needs to be agreed at the governmental level to address data sharing based on today's realities, rather than yesterday's ideals.
- The Internet has become an important trade route for the 21<sup>st</sup> Century, but there is a rising threat of "digital protectionism".
- Any international agreements should create rules to enable the cross-border flow of data to support trade and investment, while protecting personal data. Agreements of this nature take many years to negotiate and can establish rules that are in place for decades, so they need to be "future proof".
- Where trade agreements include provisions for the fundamental freedom of cross-border data movement, they must be fit for purpose if they are to gain business support and remain relevant for the digital economy.

### **Oversight/governance**

- Data controllers are responsible and accountable to regulators, clients and consumers for their handling of personal data according to the risks and realities of their business model, and legislation should be flexible enough to support different models of oversight and governance which reflect different uses of data. The realities of their business model need to be reflected, making a "one size fits all" approach unworkable across the myriad of business models and realities, including cultural differences.
- Customers, whether consumers or corporates, benefit from a flexible accountability model which leverages data and models to offer cost effective and suitable products and services to customers, and which is based on the risk of harm or loss to the customer, as opposed to a rigid one size fits all approach.
- Data rules should support organisations in using data to assess risks and to offer appropriate services to customers, whether insurance or other financial products. Focussed use of data in this way can lead to tangible benefits to customers including lower premiums and personalised products more suited to their needs.

### **Sanctions & Enforcement**

- Sanctions are an essential part of enforcement, and the level of sanctions must be proportionate to the harm actually incurred. The current focus in the draft EU Data Protection Regulation on fines, ignores the importance of allowing enforcement authorities to impose sanctions which fit the breach and are proportionate to the level of distress/damage caused. For example, a requirement of an undertaking from a CEO can be far more effective in ensuring future compliance, than a fine in many instances.
- Meaningful enforcement suitable to a dynamic environment is needed, not a blunt instrument. Enforcement should be proportionate and encourage transparency and engagement, working with the grain of concerns shared by business and consumers - business concern to safeguard data for reputational reasons, and consumers' desire for a regime that allows consumers a choice of safeguards and a degree of choice as to how they operate.
- The reality is that Community primary legislation must resist being prescriptive and overly specific in order to ensure that it is, and can remain, relevant and workable.

### **Conclusion**

Global engagement on data issues is needed to reflect the realities of the 21<sup>st</sup> century. International companies engage and do business according to global international standards, which are often higher than specific local requirements, hence supporting the accountability model, role modelling and interoperability aims (e.g. Binding Corporate Rules, Berne Convention). This means that legislative developments need to be flexible enough to recognise key distinctions, such as differences between regulated and unregulated sectors, or between business and consumer interests. It is also essential for governments and regulators to work together to acknowledge the reality and adequacy of different standards and approaches to data sharing regimes and ways of achieving a compliant approach.

**June 2014**