Ministry of Justice review of the balance of competences: call for evidence on the balance of competences between the UK and the European Union in the area of information rights.

The **BBA**, the **Association for Financial Markets in Europe** (AFME) and the **International Regulatory Strategy Group** (IRSG) welcome the opportunity to comment on Balance of Competences Review in Information Rights. Our respective trade associations represent a broad array of European and global participants in the retail and wholesale financial markets. Our members comprise pan-European Union ("EU") and global banks as well as key regional banks, wealth management firms, brokers, law firms, investors and other financial market participants. Our perspective stems from our experience of protecting the personal data of millions of customers; it also draws on the European experience of our Members, and so gives us the scope to provide unique insights on financial services policy making in Europe.

Consultation questions

1. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) has been advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

The Data Protection Directive makes reference to allowing public access to information from public bodies. Financial services firms are ultimately responsible if any of its customer information is placed into the public domain. This means that when private firms provide information to public bodies (e.g. regulators, tax authorities etc), they must be sensitive to their role as data provider/controller, as there is a high risk that this information may eventually become public. Our concern is whether EU institutions and Member States' public bodies are taking appropriate steps to ensure that appropriate provisions are in place to protect sensitive customer information from Freedom of Information Act (FOIA) and other similar requests.

For example, information provided to the Financial Ombudsman Service (FOS) does not have an automatic exemption in the way that data provided to the Financial Conduct Authority (FCA) does (under the Financial Services Markets Act (2000) (FSMA)).

Benefits to individuals - The manner in which the EU Data Protection Directive has been transposed into UK law has benefited individuals in the UK in relation to the protection of their personal data by others.

Detriment to business - However, there needs to be a balance struck between the benefits to individuals and the detriment to organisations that necessarily ensues from those rights being granted. In the UK, the impact of the EU's competence in the area of data protection has been most evident in relation to international transfers of personal data. The prohibition on data transfers, unless there is adequacy by the recipient country or one of the exemptions in the Directive is met, has by and large, been disadvantageous to business. There has been too much emphasis on 'ticking the box' by employing Model Clauses in the absence of adequacy, to the detriment of ensuring meaningful measures of accountability are in place. The application of data transfers rules, based on jurisdictional boundaries, is not effective in the context of distributed networks and complex computer environments.

International Data Flows - Furthermore, the current approach does not reflect the reality of international business data flows, online commerce or social media tools.

Member State interpretation - The options provided by the EU Data Protection Directive, and the range of approaches in this area taken by the Member States, creates confusion and complexity. In this respect, the EU's competence has not assisted businesses or other groups in the UK.

2. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) strikes the right balance between individuals' data protection rights and the pursuit of economic growth?

Balancing rights of individuals with economic growth - The rights provided to individuals in the EU Data Protection Directive largely strike the right balance between data protection rights for individuals and the pursuit of economic growth. However, the exercise of the EU's competence in these areas respects should not place large administrative and overly prescriptive burdens on firms (e.g. notification regimes, prescriptive privacy notice formats, restrictions on the ability to utilise efficiencies in cloud services etc). These costs of business inhibit growth and preclude businesses from entering into new markets or act as a barrier to entry for new firms.

Responding to data requests - There are also some areas – such as the very broad right of subject access, where the burden of responding to requests can have a significant financial impact on public and private sector organisations. This can occur when individuals believe they are providing information to a single firm, but then this information is shared with public bodies (e.g. information to regulators, tax authorities etc). The proposed EU DP Regulation contains rights for individuals which are considerably more wide ranging – for example the right to object in relation to various aspects of personal data processing – and could place more significant restrictions on the pursuit of economic growth.

Incentive-based approach - Generally speaking, the EU needs to exert its competence through the EU DP Regulation by taking an incentive-based approach to compliance with data protection requirements instead of simply relying upon penalties and enforcement measures.

Data transfers - As per the response to Question 1, the EU's competence is most obvious in relation to the current and proposed limitations on the transfers of personal data. Under the EU DP Regulation it is also important that the EU exercises its competence over international data transfers in a manner that facilitates transborder data flows to reflect existing realities around gloabalisation and digitalisation, while providing a robust framework for data protection.

3. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) is meeting the challenges posed by the increasing international flow of data, technological developments, and the growth of online commerce and social networks?

We believe there are several barriers preventing the EU from meeting the challenges posed by the increasing international flow of data, technological developments, and the growth of online commerce and social networks

Member State interpretation - There is a difficulty with the effect of EU competency in data protection because the EU Data Protection Directive has been interpreted differently in different Member States. This is not working very well given the current challenges, and also interlinks with our view on the Transatlantic Trade and Investment Partnership in question

11. For example, in some Member States approval is required for data transfers to jurisdictions without adequacy, and in others it is not.

Extraterritoriality - The EU's exercise of its competence extraterritorialy and the over-concern with geographical constraints on data processing is not aligned with the reality of data flows and the growth of online commerce, cloud computing and social media. These issues extend beyond geographical boundaries and are not being factored into legislative/regulatory developments.

New legislative/regulatory developments - The emphasis of new legislative/regulatory developments is on stopping data flows rather than enabling them, albeit in a suitable and regulated fashion. Firms need the EU to work collaboratively with other jurisdictions and regions (e.g. APEC) to develop internationally recognised codes of practice for data handling. This would enable the EU to promote standards at an international level, and so create greater certainty and consistency for firms and individuals.

Flexible legislation is needed - Data controllers are responsible and accountable to regulators, clients and consumers for their handling of personal data according to the risks and realities of different business models; legislation should be flexible enough to support different models of oversight and governance which reflect different uses of data. The realities of business models needs to be reflected, making a "one size fits all" approach unworkable across the myriad of business models and realities, including cultural differences.

Customers, (both consumers and 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.

Current examples of international codes of practice in this area include: Safe Harbour, Terrorist Finance Tracking Programme (TFTP), the Passenger Name Record Agreement, and the APEC Privacy Framework (in relation to Binding Corporate Rules).

Principles-based approach - The EU needs to exert its competence over data protection using a principles-based approach as opposed to applying detailed rules which quickly lose their relevance given rapidly developing technology in these areas. In short, there is no evidence of the EU's competence assisting growth;

- Supporting meaningful measures giving effect to growth;
- in a coherent and realistic approach to those areas impacted by the Data Protection Directive.

4. What evidence is there that proposals for a new EU Data Protection Regulation will be advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

A principal concern is that the proposed Regulation goes well beyond the prescribing of <u>what</u> must be done by firms, to prescribing <u>how</u> they must achieve this, which removes the technological neutrality and creates an unsuitable "one size fits all" approach to data protection. The risks can be summarised as follows:

Risks for financial institutions and customers all over the EU:

Difficulties in disclosing information to courts or authorities or complying with legal / regulatory obligations outside of the EU - Unless there are mutual legal assistance treaties in place, international banks and financial institutions based in the EU and UK based banks and financial institutions with overseas facilities, will not be able to comply with data requests from foreign courts, authorities or regulators.

Difficulties in sharing personal data outside of the EU – The mechanisms that allow EU based firms to share data outside of the EU will become more restrictive and are inconsistent with the needs of a global economy operating in the digital/online world. Non-EU competitors will be able to launch products and services more quickly, whilst EU companies are burdened with additional bureaucracy and the need to seek authorisations from understaffed and budget constrained data protection authorities.

Deluging customers with notices – Many of the proposed requirements to notify customers, and the level of detail required are unlikely to be of benefit to the customer, potentially leading to confusion, notice fatigue, and undue concern for customers.

Specific risks for UK based financial institutions and their customers:

Restricting the ability to make sensible business decisions through profiling customer data - The financial services industry is concerned that an unintended consequence of the Regulation means they will be unable to profile data, including sensitive personal data, for legitimate business reasons, such as anti-money laundering and anti-terrorism detection and credit assessments.

Clarity is required to understand if financial institutions will be hindered in their ability to protect customers from financial crime. The financial services industry is concerned about unintended consequences that both the European Parliament (EP) and Council drafts permit data processing only if there is a Member State or EU legal obligation to do so. FCA rules and regulations, as well as international standards (e.g. FATF) are not strictly Member State or EU legal obligations and would not therefore be caught by this legitimate ground for processing. Financial institutions would therefore have to rely on another ground to legitimise the processing to comply with regulatory obligations, international standards and best practice; furthermore it is not clear what this basis for processing would be.

Financial Institutions will have difficulty passing data to Credit Reference Agencies ("CRAs") to conduct credit checks – Related to the above issue of complying with legal obligations, financial Institutions do not have a specified "legal ground" to pass customer data onto 3rd parties, such as CRAs. Once again, the trade associations appreciate that there is no intended consequence of the text to prohibit credit checking; however clarification of the Regulation's impact is needed to understand if there will be any impact on our members' ability to credit check and lend responsibly. For example, would it be considered in the institutions' legitimate interests to share data with credit reference agencies?

5. What evidence is there that the right to access documents of the EU institutions has been advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

Some disadvantages have been observed by firms in that the ability to access official documents needs to be in a manner that:

- does not prejudice official public business or place an undue burden on official institutions;
- does not place a large financial burden on business;

- does not prejudice the rights of other citizens.

Freedom of Information Act (FOIA) Due to requirements under FOIA, firms need to consider whether customer information should be redacted before it is shared with the regulator.

As a consequence, firms may be removing information that might be helpful to regulators and other public bodies, through being over cautious about the future use of that data, which may negatively impact transparency (ie full disclosure). The right to access public documents means that financial services firms are ultimately responsible if any of their customer information is placed into the public domain. This means that when private firms provide information to public bodies (e.g. regulators, tax authorities etc), they must be sensitive to their role as data provider/controller, as there is a high risk that this information may eventually become public.

Our concern is whether EU institutions and Member States' public bodies are taking appropriate steps to ensure that appropriate provisions are in place to protect sensitive customer information from FOIA and other similar requests.

For example, information provided to the Financial Ombudsman Service (FOS) does not have an automatic exemption in the way that data provided to the Financial Conduct Authority (FCA) does (under the Financial Services Markets Act (2000) (FSMA.))

6. How would UK citizens' ability to access official information benefit from more or less EU action?

All action should have the underlying premise of encouraging economic growth and protecting the use of individual's information.

7. How could action, in respect of information rights, be taken differently at national, regional or international level and what would be the advantages and disadvantages to the UK?

We do not wish to provide any comments at this stage

8. Is there any evidence of information rights being used indirectly to expand the competence of the EU? If so, is this advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

We do not wish to provide any comments at this stage

9. What is the impact on EU competence of creating an entirely new legal base for making data protection legislation that is not expressly linked to the EU's single market objectives?

Granting the EU competence to act on data protection as a subject in and of itself means that the assertion of that competence will not be based simply on the free movement of goods and the philosophy of the single market. As such, depending upon the exercise of the EU's powers through its institutions, the prioritisation of data protection could increase relative to the assertion of other legal rights.

Organisations need a consistent and clear mechanism in order to determine the requirements for data protection, in particular the requirements for protecting data transfers which need to be facilitated and not simply prohibited.

An entirely new legal base that is not linked to the single market creates a consistently conflicting regime where privacy and economic growth / the digital agenda, are too often in conflict for firms looking to operate across and beyond the EU. The single market encourages transfers which in turn encourages business.

10. What future challenges or opportunities in respect of Information Rights might be relevant at a UK, EU or international level; for example cloud computing?

Opportunities of the Internet and mobile technologies, and globalisation

The Internet, Mobile technologies and the phenomenon of globalisation facilitate 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 organisation 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.

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, as provided for in the draft EU Data Protection Regulation.

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 21st century.

While data protection and security are essential, cross-border 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 in individual jurisdictions is recognised as important and legitimate to safeguard society and to counter crime and terrorism. However, this requirement needs to be met at the government/public sector level, and not through the imposition of data restrictions on the private sector; such restrictions cannot guarantee access to data for a Government or relevant authority, but instead create risk by introducing conflicting obligations for firms. Increasingly, too, the public sector obliges the private sector to collect and process data on its behalf to comply with innumerable reporting and transparency obligations (eg tax). Rules on access to data for Government and relevant authorities need to steer carefully between the potential conflicts inherent in this web of differing needs, which cannot be resolved simply by placing added requirements on the private sector.

Free flows of data are particularly important to guarantee the ability of firms to carry out intra-company data transfers across businesses operating in many 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. For more information, see Question 11on TTIP.

International Support for Digital Trade

A global solution focussed on mutual recognition needs to be agreed to address data sharing based on today's realities, rather than yesterday's ideals.

The internet has become an important trade route for the 21st century, but there is a rising threat of "digital protectionism".

Any international agreements relating to information rights 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".

Sanctions & Enforcement

Sanctions are an essential part of enforcement, and the level of sanctions must be proportionate to the harm actually incurred or the potential risk of harm.

Meaningful enforcement suitable to a dynamic environment is needed, not a blunt instrument. Enforcement should be proportionate and encourage transparency and engagement, working –with 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.

Global engagement on data issues is needed to reflect the realities of the 21st century. Global firms 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 support greater harmonisation and recognition of standards that impact organisations operating across multiple jurisdictions, which is the reality of today's world.

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.

11. Is there any other evidence in the field of EU Information Rights that is relevant to this review?

The implementation of other legislative instruments by the EU needs to take into account its competence in relation to data protection and information rights so that this competence is

reflected directly in the drafting and there is meaningful linkage/ interaction between the key policy principles of these related legislative instruments. EU institutions may have responsibility on issues that are related to Data Protection / Information rights but they are not factoring in these concerns into the legislative drafting. The consequence is that there is confusion and conflict between obligations making it difficult for organisations to interpret and implement.

An example is the 4th EU Anti-Money Laundering Directive and the proposed EU Data Protection Regulation, neither of, which have been drafted in consideration of the other, as their approach to data use is opposing in many instances (eg, data minimisation vs data maximisation).

How the EU's competency will be applied through institutions, such as the European Data Protection Board, and through derogations of power to the Commission need to be clear under the EU Data Protection Regulation. The concentration in and centralisation of, EU competencies within these institutions leads to problems with creating legally binding instruments that apply broadly to all data protection issues without considering highly regulated industries or other industry-specific issues. The power of these institutions needs to be exercised appropriately in a principles-based manner, particularly in relation to data transfers. Firms need mechanisms for transfers to flow easily so that commerce and growth are not delayed or hindered.

From a broader perspective, it is important to note the cross-cutting nature of the current Transatlantic Trade & Investment Partnership (TTIP) negotiations and in particular its political (though not formal) links with EU Information Rights issues. It is noted that the US has a strong interest in reaching a common understanding with the EU on data protection questions. It is important that any advances made on EU developments are not hampered by negotiations on other politically sensitive topics within TTIP, and that the overall balance of interests is not lost sight of as the negotiations proceed.

ENDS