BALANCE OF COMPETENCES REVIEW: MINISTRY OF JUSTICE CALL FOR EVIDENCE ON INFORMATION RIGHTS

INTRODUCTION

RSA Insurance Group welcomes the opportunity to provide evidence to the Ministry of Justice's (MOJ) Call for Evidence on Information Rights.

Both the freedom of establishment and freedom of services principles enable us, as a European and global insurer, to effectively operate and write business in a number of European countries. With this in mind, being part of the EU is crucial for RSA. It provides us with the gateway to trading with the rest of the world. Having 500 million consumers on our doorstep is beneficial for companies like RSA and having us trading here is good for consumer choice and competition. Advancing the Single Market should be a priority objective for EU and UK policy development.

However, with 90% of global growth happening outside the EU, we do believe that the EU needs to become more competitive and be open to business from outside its borders. This is equally true for data flows which, also increasingly, need to be global.

ABOUT RSA

With a 300-year heritage, RSA Insurance Group is one of the world's leading multinational insurance groups. RSA operates solely in the non-life insurance market across 32 countries and we provide products and services in over 150 countries world-wide. Across Europe, RSA has businesses currently selling personal lines insurance (e.g. motor, home and pet insurance) and commercial insurance (e.g. marine, renewable technology, construction and engineering) in the UK, Ireland, Sweden, Denmark and Italy. We also have branches in Germany, France, Spain, Netherlands and Belgium, from which we provide large scale commercial insurance.

We have developed and implemented a robust Group Data Protection Policy and Data Protection Compliance Framework, which has been rolled out globally, in conjunction with a network of data protection oversight owners appointed locally in each country. The purpose of our framework is to equip countries to effectively implement data protection legislation to consistently maximise the protection of personal data, which in turn minimises the risk of breach and sanction. Our framework reinforces the necessity for accountability in each country.

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?**

Member States have flexibility in implementing the EU requirements under the 1995 Directive. In the UK, this has resulted in a risk-based approach, which balances the rights of data subjects with the ability of businesses to operate effectively and meet the needs of their customers. This is advantageous to both individuals and businesses.

However, we do see a difficulty with cross-EU competencies in data protection as issues are interpreted differently in different countries. RSA therefore supports the overall purpose of the proposed Data Protection Regulation and the European Commission's aim of creating a level playing field, holding data processors more directly accountable and making data protection officers mandatory as this materially strengthens the data protection profile in terms of corporate governance.

As a data controller under the current Directive, RSA is responsible if any of its customer personal data is placed into the public domain. This means that when/if we provide information to public bodies, for example, regulators or tax authorities, there is a high risk that this information may eventually become public. It is imperative that under the current review of the 1995 Directive this personal/sensitive data is adequately protected. EU institutions and Member State Governments must therefore take the necessary steps to ensure that appropriate provisions are in place to protect personal/personal sensitive data from Freedom of Information Act (FOIA) and other similar requests.

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?

We believe that private businesses can play an important role in ensuring that the UK continues to reap the benefits of EU membership as well as the role businesses play in securing economic growth. As such, any balance between individuals' data protection rights and the pursuit of economic growth should not place excessive financial and administrative burdens on firms, for example, excessive notification regimes or prescriptive privacy notice formats. These costs to business inhibit growth and act as a barrier.

Similarly, when drafting new legislation, the EU should have more regard for the impact that regulatory proposals have on the competitive position of EU firms. Overly prescriptive legislation can put them at a disadvantage to their global counterparts, also risking regulatory arbitrage.

The EU also needs to take competition and the growth agenda into account when drafting legislation to address an issue in a different sector. For example, the proposed Data Protection Regulation aims to fix problems associated with social media, however the catch-all principle of the proposed Regulation means that it can have a negative impact on insurers, for example, it could prevent insurers pricing risk appropriately and take away the competitive elements relating to customer service, policy cover and claims management. This would have a fundamental impact on how insurers operate and write business, demonstrating the Commission's often piecemeal approach, which does not take in to account the full set of consequences. This is where we can see that the balance is in favour of individuals' data protection rights rather than the pursuit of economic growth.

We would encourage the Directorates General to take a more coordinated approach to policy-making or shared responsibility for a piece of legislation which has a major impact on more than one sector.

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?

There is no evidence to support this and the current emphasis of the proposed new Data Protection Regulation does not take into consideration the 'globality' of 21st century data flows, for example social media, cloud computing. This is despite the stated aim of the Commission to update the 1995 Directive and bring legislation up to date. Please also see our response to question 10.

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?

RSA supports the Commission's aim of creating a level playing field for data protection across the EU and we believe this will be most appropriately achieved through a Regulation. In our view the Regulation has the potential to deliver an effective and practicable system of data protection. However, while some of the provisions go some way towards reducing the administrative burden for organisations, there are other proposed amendments that would significantly increase this burden as well as the costs of providing insurance cover in some cases; and some that would significantly change the way in which insurers operate.

All of this goes against the Commission's aim of delivering a standard and effective regulation across the EU. In our view, a risk based approach should be adopted so we continue to see a balance between the rights of individuals and the ability of businesses to operate effectively and meet the needs of their customers. As currently drafted, the Regulation is very prescriptive in a number of areas.

For example, the Regulation, as drafted by the European Commission, would impact on the ability of insurers to share information to prevent fraud and other financial crime. Detecting fraud protects consumers and reducing and deterring insurance fraud is a priority for the insurance industry. It is important that efforts to combat fraud (which are in the overriding interests of society) are supported and explicitly recognised in the development and application of the law, rather than being restricted. At the moment, insurers are able to share sensitive data under UK law, which is possible under the 1995 EU Directive, which only sets down minimum harmonising standards. This is an example of where a proposed maximum harmonisation approach presents an obstacle to a national objective, namely fraud prevention. We believe that fraud prevention is still possible under a Regulation but the Commission should have taken into account such practices and processes in its drafting.

The proposed Regulation not only prescribes what must be done by data controllers but also how it must be achieved. This throws up a number of issues such as:

a) Sharing personal data outside of the EU will become more restrictive. Non-EU businesses will be in a position to launch products and services far more expediently, while EU companies will be burdened with additional bureaucracy and the need to seek authorisations from Data Protection Authorities.

b) Mandatory breach reporting – the requirement for businesses to report all breaches to Data Protection Authorities will become an unwieldy administrative burden for both parties. No level of materiality has been factored in to when breaches must be notified. Reporting all breaches, including the most trivial, will prove impossible to manage.

c) Breach notifications to customers will increase and require to become more detailed and frequent, potentially resulting in undue and unnecessary customer confusion and/or concern and ultimately notification fatigue.

d) We are concerned that an unintended consequence of the proposed Regulation will be the inability to profile personal data for legitimate business purposes such as underwriting and for the prevention and detection of fraud. Underwriting is the key element in the insurance risk profiling process, without which RSA cannot function as an insurance provider.

e) FCA/PRA regulations are not legal obligations and so may not be classed as a legitimate ground for processing, thereby not allowing processing to comply with regulatory obligations.

The proposed Regulation is an example of legislation which does not always respect the principles of proportionality and subsidiarity. As currently drafted, it is likely that the cost of implementation will exceed the intended benefit. Too much focus on the granular can reduce requirements down to a tick box exercise for organisations and Data Protection Authorities alike, rather than focussing energy and resource on good data protection practices. There is a danger that measures designed to help individuals manage their data more effectively will have a disproportionate impact on businesses.

RSA would argue that not respecting the principles of proportionality undermines the Single Market: disproportionate legislation hinders competition and does not allow companies to operate effectively across borders with overly burdensome rules constituting a de-facto barrier to entry and competition. The UK Government must help to ensure the insurance sector is seen as a key driver of European economic recovery; that EU firms retain their global competitive advantage and that the regulatory burden being imposed on the insurance industry does not become too excessive and disproportionate

Linked to the above is that RSA believes there should be a requirement for thorough cost benefit cases to be undertaken involving real industry analysis. It is important that the full cost to industry is understood, for example, the cost and timeline to make major system changes when changes to documentation are required. Ultimately an increase in the cost of compliance feeds through to the price customers pay. In our view the European Commission does not perform enough cost benefit analyses ahead of proposing new legislation andRSA believes the European Commission should measure the impact of regulations and take a risk-based and proportionate approach when developing new proposals. If EU businesses are to compete in the global marketplace, they need a level playing field.

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?

The EU Institutions, in particularly the Council, have become much better at sharing official documents on a timely basis. This open and transparent culture should be encouraged as it is a helpful tool for businesses, such as RSA, to keep track of progress of legislation and for understanding the impact, cost and timing of the policy on our business and customers.

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

No comments.

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?

No comments.

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?

No comments.

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?

Firms need a consistent mechanism to facilitate easier data transfers. An entirely new legal base that is not linked to the EU's single market objectives would not be preferable for global firms looking to operate across the EU. As noted earlier in our response, RSA uses the freedom of establishment and freedom of services effectively to allow us to operate and write business in a number of EU Member States. The Single Market encourages transfers which in turn encourages business and growth. This should be a key objective for the EU's next five year mandate.

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?

Appropriate technical and organisation measures are vital to safeguarding personal data in a fast evolving environment - one where customers continue to demand bespoke on-line services and are increasingly technically savvy across all generations.

It is inconsistent to encourage global expansion on one hand and yet restrict data-flow requiring localisation of data-processing and inhibiting compliance with requirements of foreign jurisdictions on the other. Global flows of data are becoming the norm and geographical restrictions are becoming obsolete as they no longer reflect current concepts of data movement and data sharing or the realities of commercial datause in the 21st century.

While data protection and security are essential, cross-border restrictions on processing and sharing data stifle 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.

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 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.

Data controllers are responsible and accountable to their customers and their regulators for the processing of personal data within risk appetite as per their business model. DP law should therefore be sufficiently flexible to support different models of oversight and governance which reflect the different uses of personal data. Our customers, whether consumers or other businesses, benefit from a flexible accountability model which leverages data to offer cost effective and suitable products and services to customers.

Sanctions are an essential part of enforcement and the level of sanctions must be proportionate to the actual harm incurred or the potential risk of harm. This is not the case with the current proposed Data Protection Regulation.

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

When proposing new legislation, it is important for the Commission to also take into account other proposed or existing legislation, otherwise a conflict in law is created which is difficult for firms to interpret and implement. Examples of regulatory overlap include:

- The 4th EU Anti Money Laundering Directive and the proposed EU Data Protection Regulation; and
- The EU e-Privacy Directive (D2002/58 on Privacy and Electronic Communications) and the proposed Data Protection Regulation.