House of Commons

Justice Committee

The Committee's opinion on the European Union Data Protection framework proposals

Third Report of Session 2012–13

Volume II

Additional written evidence

Ordered by the House of Commons
to be published 4 & 17 September 2012

Published on 1 November 2012
by authority of the House of Commons
London: The Stationery Office Limited

The Justice Committee

The Justice Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Ministry of Justice and its associated public bodies (including the work of staff provided for the administrative work of courts and tribunals, but excluding consideration of individual cases and appointments, and excluding the work of the Scotland and Wales Offices and of the Advocate General for Scotland); and administration and expenditure of the Attorney General's Office, the Treasury Solicitor's Department, the Crown Prosecution Service and the Serious Fraud Office (but excluding individual cases and appointments and advice given within government by Law Officers).

Current membership

Rt Hon Sir Alan Beith (*Liberal Democrat, Berwick-upon-Tweed*) (Chair)
Steve Brine *(Conservative, Winchester)*
Mr Robert Buckland (*Conservative, South Swindon*)
Jeremy Corbyn (*Labour, Islington North*)
Nick de Bois (*Conservative, Enfield North)*
Christopher Evans (*Labour/Co-operative, Islwyn*)
Ben Gummer (*Conservative, Ipswich*)
Rt Hon Elfyn Llwyd (*Plaid Cymru, Dwyfor Meirionnydd*)
Seema Malhotra (*Labour/Co-operative, Feltham and Heston)*
Yasmin Qureshi (*Labour, Bolton South East*)
Elizabeth Truss (*Conservative, South West Norfolk*)
Karl Turner (*Labour, Kingston upon Hull East*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the internet via www.parliament.uk.

Publication

The Reports and evidence of the Committee are published by The Stationery Office by Order of the House. All publications of the Committee (including press notices) are on the internet at www.parliament.uk/justicecttee.

The Reports of the Committee, the formal minutes relating to that report, oral evidence taken and some or all written evidence are available in a printed volume. Additional written evidence may be published on the internet only.

Committee staff

The current staff of the Committee are Nick Walker (Clerk), Sarah Petit (Second Clerk), Gemma Buckland (Senior Committee Specialist), Helen Kinghorn (Committee Legal Specialist), John-Paul Flaherty (Committee Specialist), Ana Ferreira (Senior Committee Assistant), Miguel Boo Fraga (Committee Assistant), Greta Piacquadio (Committee Support Assistant), George Margereson (Sandwich student), and Nick Davies (Committee Media Officer)

Contacts

Correspondence should be addressed to the Clerk of the Justice Committee, House of Commons, 7 Millbank, London SW1P 3JA. The telephone number for general enquiries is 020 7219 8196 and the email address is justicecom@parliament.uk

List of additional written evidence

List of unprinted written evidence

The following memorandum has been reported to the House, but to save printing costs it has not been printed and copies have been placed in the House of Commons Library,

where they may be inspected by Members. Other copies are in the Parliamentary Archives, and are available to the public for inspection. Requests for inspection should be addressed to The Parliamentary Archives, Houses of Parliament, London SW1A 0PW (tel. 020 7219 3074). Opening hours are from 9.30 am to 5.00 pm on Mondays to Fridays.

Hargreaves Lansdown

Written evidence

Written evidence from the Brussels European Employee Relations Group

PROPOSED EU GENERAL DATA PROTECTION REGULATION (2012/0011)

EXECUTIVE SUMMARY

— Business needs certainty and practicality from the legislation under which it operates. There are many varied and different personal data processing regimes across the EU.

— Such complexity already places the EU at a competitive disadvantage in attracting employers and encouraging job growth and economic development.

— BEERG welcomes the idea of a Regulation—one set of clear and precise data protection laws to cover all EU and EEA members.

— Employee personal data is a special and distinct category of personal data. Processes and procedures that are appropriate for customer or client data are inappropriate for employee data. Multinational companies need to be able to manage multinational workforces and to be easily able to access personnel data to do this.

— We believe the proposed General Data Protection Regulation (GDPR) (2012/0011), as presented:

  — Fails to recognise the unique nature of personal employment data; and

  — Fails to strike a balance between the need to provide reasonable protection for the personal data of the individual with the unavoidable needs of business to be able to operate in an effective manner.

SPECIFICALLY

— Article 82 of the GDPR completely undermines the concept of a Regulation by allowing Member States to adopt rules additional to those already spelt out in the Regulation as regards employees' personal data.

— The Article 7 consent of employees provisions are overly restrictive., The consent of employees, or prospective employees, for such personal data processing as is essential to the employment relationship should be taken as a given.

— Requiring the appointment of data protection officers in all organisations with more than 250 employees is both unnecessary micromanagement and a major additional cost that would place the EU at an even greater competitive disadvantage.

— The Communication of Personal Breach requirements in the employment context are excessive and the proposed penalties proposed under the Regulation are too harsh without any element of proportionality.

— We are deeply concerned by the very broad powers the Regulation gives the Commission to adopt secondary acts without full, transparent democratic oversight or consultation with the social partners.

INTRODUCTION

1. The Brussels European Employee Relations Group (BEERG) provides a forum for European employee relations specialists and in-company employment lawyers to discuss issues of mutual concern. We have over 60 major transnational corporations in membership. We work closely with the Washington DC-based HR Policy Association. Together we work with over 300 major multinational corporations employing over 25 million workers globally.

2. Business needs certainty and practicality in the legislation under which it operates. At present, there are different regimes applying to personal data processing in different European Union Member States, with differences in the rules and their policing. This is problematic and threatens to become more so as several countries revise their approach to data protection to deal with the major developments in technology and behaviour since the original Data Protection Directive.

3. Accordingly, we welcome the idea of a Regulation—one set of clear and precise data protection laws to cover all EU and EEA members.

4. The European Union is rightly concerned that personal data exported outside the jurisdiction might be misused and therefore insists on safeguards before allowing its export. However, the discussion and attention around the proposed Regulation appears to have overly centred on issues relating to social media business and not the vast number of other types of business.

5. Our concern is with the rules regarding the personal data which business is obligated to hold and process in order to employ an EU workforce. Common to all businesses, and which needs to be discussed and addressed separately within the Regulation, is the need they all have to process employee personal data. Many also transfer such data from the EU to third countries. This is increasingly the case as more and more businesses make use of the enhanced processing capacity that "cloud computing" offers.

6. Employee personal data is a special and distinct category of personal data. The proposed regulation should recognize that basic employment data must be collected and utilized, and relieve employers from the same prerequisites and restrictions imposed for collecting and using consumer data, as long as employers follow a basic set of rules. It is inequitable and impracticable to lump together the concerns relating to data privacy and new social media with the data processing that every business must do on the employment relationship: hiring people, managing them and dealing with their departure.

Article 82

7. In the area of most concern to us, employment related personal data, Article 82 completely undermines the concept of a Regulation by allowing Member States to adopt rules additional to those already spelt out in the Regulation as regards employees' personal data. For multinational enterprises operating across Europe this may mean having to eventually comply with the Regulation and 27 different sets of domestic employment related data protection laws. Such complexity already places the EU at a competitive disadvantage in attracting employers and encouraging job growth and economic development against those world areas without such difficult and complex laws. We believe that Article 82 should be dropped completely and replaced by a specific chapter on the processing of employment-related personal data.

Article 7

8. The "consent" requirements (Art. 7) for employment related personal data in the Regulation are overly restrictive. There is, or should be, an understanding in the Regulation that the gathering, processing, and retention of relevant employee personal data by the employer is an essential part of an employment relationship, and should permit employers to do so as long as such data is used responsibly and that reasonable remedies exist should that trust be broken.

9. We believe that the consent of employees, or prospective employees, for such personal data processing as is essential to the employment relationship should be taken as a given. Management should not be required to ask for consent or file administrative registrations every time it is necessary to make changes to a company's human resource related personal data processing systems.

10. If it is felt necessary to establish some general ground rules, we would favour the development of a "model employee personal data protocol" covering basic and essential data processing which would form an (express or implied) appendix to all employment contracts. Such a "protocol" could cover not only essential employee personal data but also potential modifications to essential HR data, email and IT security initiatives. It could form an appendix to, or a separate chapter in, the proposed Regulation. There will, of course, be differing views as to what is essential and non-essential employment data, but we believe that a consensus could be found which would allow businesses to function effectively while safeguarding the rights of employees.

11. Processes and procedures that are appropriate for customer or client data are inappropriate for employee data. Multinational companies need to be able to manage multinational workforces and to be easily able to access personnel data to do this. Existing regulations and practices across Europe make this impossibly complex, with a potentially adverse impact on employment. A protocol along the lines suggested above could also cover the issue of the transfer of employee data outside the EU to other affiliates within the same company or group which is centrally managed and to outside contractors that the company may use to manage or process such data. Such a "protocol" could also relieve companies of the necessity of having to apply to the national data processing authorities every time they want to change or upgrade human resource data systems, or transfer data outside of the European Union. At present it can take several years for the national authorities to agree to such changes or transfers.

12. The protocol we suggest as a better way forward could build further on existing practices such as "binding corporate rules" and "standard contractual clauses", while still holding global organizations firmly responsible for misuse of such data. It should state broad principles, with appropriate penalties for their breach, rather than seek to micro-manage every company's processing of employee personal data. EU health and safety law, which rightly concerns workers and their families much more than personal data management, do not require companies to have prior approval from national health and safety authorities for their health and safety policies: but employers are made subject to significant sanctions if they are found to be in breach of the law. This seems to us a better approach.

Other Areas

13. We also have concerns about the requirement to appoint data protection officers in all organisations with more than 250 employees. We believe that a requirement to appoint data protection officers would likely prove both expensive and less effective than having companies take responsibility for their obligations in whatever manner works best for their operating structure. Why not simply require compliance with the Regulation, allowing employers to take responsibility for how they achieve compliance, against a backdrop of suitable sanctions (fines) for non-compliance or breach?

14. The Communication of Personal Breach requirements in the employment context are excessive. Employers should be allowed to fulfil their communication requirements to employees with general notices to

all EU employees en masse using whatever means is reasonable and on practicable timescales. Setting timescales of 24 hours for Notifications to Supervisory Authorities is not practicable, and overhasty Notification runs the risk of further error or misleading messages.

15. The penalties proposed under the Regulation are too harsh without any element of proportionality. Penalties should be calibrated to the amount of harm caused by a violation, and whether the violation was intentional. A percentage of revenue approach is wrong.

16. This is a fast-moving field and the Commission understandably wishes to be able to keep up with developments. When the Data Protection Directive was adopted in 1995 business was nowhere near as global as it is today. It is, however, important that future revisions of rules to meet new challenges should be realistic and practical. They should be subject to the same consideration by the wide range of stakeholders as normal EU legislation. In the case of changes to the provisions applying to personal data held on employees, which is effectively employment law, this means the social partners. We are particularly concerned by the very broad powers the Regulation gives the Commission to adopt secondary acts without full, transparent democratic oversight or consultation with the social partners; in the case of employment-related data.

17. In conclusion, we hold that the proposed Regulation must strike an appropriate balance between the need to provide reasonable protection for the personal data of the individual with the unavoidable needs of business to be able to operate in an effective manner that allows for business development and employment growth.

18. We do not believe that the Regulation, as presented, strikes that balance.

August 2012

Written evidence from Towers Watson

EUROPEAN UNION DATA PROTECTION FRAMEWORK PROPOSALS

SUMMARY

The proposed changes to data protection legislation could potentially create challenges for UK pension schemes.

Our main concern relates to Articles 6(a) and 7 of the draft regulation, which will require data subjects to give their *explicit* consent to their personal data being processed by the data controller, ie they must actively consent to processing of their personal data. In the case of a pension scheme, the data subject is the member and the data controller is the trustees (either solely or in conjunction with a third party).

Obtaining explicit consent of pension scheme members by pension scheme trustees will be problematic for two reasons:

1. Pension schemes will need to contact all members of the scheme on the date the new data protection legislation comes into force to obtain explicit consent to process data, including deferred members for whom the scheme may not have an up-to-date address. This could be a very costly and administratively burdensome exercise for pension schemes to undertake, and raises difficulties in relation to members who cannot be traced or do not respond.
2. In relation to members who are automatically enrolled the AE legislation forbids trustees from making it a condition of membership of their scheme that employees actively consent to their personal data being processed.

This means pension schemes will need to rely on one of the other conditions in Article 6. These potentially include:

(a) "Processing of data is necessary for the performance of a contract to which the data subject is party." In relation to a pension scheme the data subject ie the employee will have a contract with the employer but not the trustees. Therefore I do not believe that trustee can use this.

(b) "Processing is necessary for compliance with a legal obligation to which the controller is subject." The requirement to automatically enrol eligible workers falls on the employer not the trustees. Pension scheme trustees do have legal obligations to retain certain information for particular members. However, these obligations are spread out over a number of regulations and it is not clear that this will encompass all members who are automatically or contractually enrolled.

(c) Processing is necessary for the purposes of the legitimate interests pursued by a controller. This would seem to us to be the most promising, since all the trustees are doing is operating the pension in accordance with the employer's wishes, and are processing personal data for the benefit of pension scheme members. However it would be helpful if either the EC or the UK government could explicitly state that this condition is met in respect of the processing of pension scheme data by trustees of the scheme.

August 2012

Written evidence from Stephanie Johnson

This is in response to a request for feedback on the proposed new EU Regulations. Whilst I support regulation to give protection to individuals the Regulation as it is currently drafted is simply going to be a very costly exercise for business to implement and contains many areas which need a lot more thought or, preferably, to be deleted eg the removal of the prescriptive requirements to maintain documentation.

Firstly the proposed 3 tier penalty structure is completely out of proportion to the type of action which might trigger a fine eg a possible fine of 0.5% of global turnover for not having some documentation which would not have any impact on a member of the public using your services is not proportionate to the infringement.

Secondly there seems to be nothing in the legislation to enable action to be taken against individuals who steal data or sell it for their own gain. That is a strange omission.

The removal of the discretion for the country's regulator to decide whether or not a fine is appropriate is a backward step. Fines should be reserved for major infringements not for every small human error.

The proposal for mandatory data protection impact assessments seems an unnecessary burden on most businesses, many of whom will have little or no impact on the general public, which presumably this legislation is meant to protect.

I'm definitely opposed to the timeframes currently being proposed for reporting data breaches. They are unrealistic and do not give time for a considered look at what has gone wrong, how it should be rectified or to accurately quantify the impact on individuals or businesses. 24 hours is going to be impossible to comply with and is simply going to lead to rushed disclosure without any idea of how the follow up matters are going to be dealt with. Not a good place to be for either the business involved or the individuals whose data may have been disclosed erroneously.

I think the right to be forgotten is also unnecessary and likely to lead to a lot of confusion amongst the general public who will probably expect a much quicker removal of their data than is likely to be the case in practice, particularly where it may have been released into the public domain. I also wonder how it will work when someone has asked to be removed from mailing lists, which keep a record of such requests, and then they ask to be forgotten so that request is also lost? It is also going to be a costly exercise to search though all data held to identify that about one particular individual and to delete it all. Also the requirement to carry out the erasure without delay is going to cause issues—it is going to be important to verify that the request has come from the data subject and that can take time along with the time to find where all the data is stored.

The other disappointment is the proposed reduction in the time period allowable to respond to subject access requests. One month is actually a very "woolly" concept given the difference in the length of some months compared to others. A specific number of days is much more sensible and the current one of 40 days is barely enough to respond to some requests now.

Also this requirement to respond to subject access requests electronically if they have been received by that medium raises a real privacy concern. How do you verify the authenticity of such a request, especially if it has come from an internet café machine or some other non recognisable ISP address. That is neither reasonable nor sensible. Also how do you ensure the data you send by this means is secure? This has not been thought through.

The proposed changes to the documentation that has to be maintained are, again, going to create additional costs and a burden on business that is not necessary, especially for the smaller businesses.

Data portability—whilst appreciating what this is trying to achieve—the current drafting leaves more questions than answers. Where will data controllers stand if the standard template that is adopted means they receive more data than they need? Another cost implication is the need for any data recipient to check what is received against what is required.

The definition of personal data is too broadly drafted. In its current format it seems to be saying that we would have to treat anonymised data as personal data if there is any likelihood a third party knows who the data subject is. If we do not know exactly who the data subject is how do we provide a fair processing notice? Again this is just not practical.

The imposition of direct responsibilities for data processors will impact on existing contracts for a lot of businesses and again this will have significant cost implications, even if you limited the costs to the time taken to negotiate new arrangements and/or amend existing documentation. Also the obligation to maintain processing records is simply going to increase the costs of storage, whether these are on paper or held electronically. Again the requirement to notify a breach immediately needs to be revised to a more realistic timeframe.

I'm also a little unclear on the requirement to appoint a data protection officer—will this be one person for a group or would every group company that employs over 250 employees have to have its own separate officer? More costs.

August 2012

Written evidence from the FLA

Executive Summary

1. The FLA is concerned by many of the new provisions proposed under the draft Regulation. In particular, the "right to be forgotten" would prevent lenders using past data to assess a borrower's creditworthiness.

2. Similarly, the proposed principles for data processing would conflict with the credit industry's commitment, under existing EU and national law and regulation, to lend responsibly and prevent fraud.

3. The proposal to make data access requests free of charge would prevent lenders legitimately charging £10 to deter claims management companies (CMCs) and fraudsters seeking to obtain high volumes of consumers' credit data.

4. The draft Regulation would also introduce new, bureaucratic and time-consuming requirements in the form of unnecessary impact assessments and inappropriately detailed new provisions on explicit consent.

5. Some of the proposals are also unclear and would, as drafted, require further explanation in the form of additional guidance. This would seem to conflict with the intended purpose of Regulations, which is to create certainty.

Introduction

6. The FLA is the leading trade association for the asset, consumer and motor finance sectors in the UK. Our members include banks, subsidiaries of banks and building societies, the finance arms of leading retailers and manufacturing companies, and a range of specialist lenders.

7. FLA members provided £73 billion of credit to UK businesses and households in 2011. Of this, £52 billion was in the form of consumer credit, representing almost 30% of UK consumer lending. £21 billion financed business equipment investment in the private and public sectors, representing over a quarter of all UK fixed capital investment. FLA members provided £20 billion of motor finance in 2011 and financed more than 60% of all new car registrations.

Data and the credit industry

8. The processing of personal information is crucial to the credit industry. Properly organised and controlled data-sharing enables lenders to make responsible lending decisions. It is clearly very important that the personal data involved is properly protected and handled so as to minimise the opportunity for fraud.

9. Like most lenders, FLA members collect and store personal information relating to their customers. This is done to the extent necessary to process an application for credit, to provide credit to the customer, and to service the credit agreement during its lifetime. The procedures are robust and kept under constant review.

10. Certain elements of this information are shared between lenders via the credit reference agencies (CRAs). These include name, address, date of birth, and payment profile. Sharing this information enables other lenders to gauge an individual's level of indebtedness and thus take responsible lending decisions. For this reason, consumer advocacy organisations support the sharing of information for such purposes. The shared information is also important in verifying an individual's identity, managing risk and minimising potential bad debt.

11. FLA members may also share information on an individual with CIFAS (the UK's Fraud Prevention Service) if that individual has undertaken a proven fraud. This is important in enabling other lenders to identify potential fraudulent applications.

Questions

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

12. We acknowledge the need to update the European legislative framework to reflect technological developments. Nevertheless, the proposals would be disproportionate for credit industry as they do not reflect market realities. Many elements of the draft Regulation would undermine the credit industry's ability to lend prudently and to minimise their exposure to fraudulent activity.

13. Under the right to be forgotten (Article 17), a consumer could demand the erasure of their credit data. Access to historic data is fundamental to responsible lending because it enables a lender to assess the borrower's creditworthiness. This new right would exclude anyone who exercised it from qualifying for a loan, as the lender would have no basis on which to make a responsible credit decision.

14. Article 5 restricts the data held to the "minimum necessary". This directly contradicts other regulatory requirements, including for example those contained in the Consumer Credit Directive and the UK Office of Fair Trading's Irresponsible Lending Guidance, which are aimed at ensuring sound lending practices.

15. Borrowers already give explicit consent to their data being used for general purposes by agreeing to a "fair processing notice" at the outset of the credit agreement. However, article 4(8) of the new Regulation suggests that explicit consent would be required from the borrower for *each* separate purpose. This would be time-consuming, resource-intensive and costly. There is also no evidence to suggest consumers would want a more detailed analysis of consent notices and this proposal could dissuade them from giving consent, thus making it more difficult for them to obtain credit. As a result of the draft Regulation, we estimate that it would cost £1.5 million to update data protection notices for a 100,000 customer base.

16. The fact that Article 6(1) does not explicitly recognize fraud prevention and detection as a criterion for lawful processing means that lenders may be unable to hold certain data to protect themselves against fraud.

17. A further problem arises from the free-of-charge access requests provided for by Article 12(4). Lenders may currently charge £10 for a subject access request (SAR). Many FLA members receive over one hundred SARs per calendar month and a significant amount of work is involved in their administration. For example, the lender may hold more than one account for the individual submitting the request, using multiple processing systems. Inevitably, any costs incurred by lenders would be passed on to consumers in the form of higher prices.

18. The existing small charge to access data acts as a deterrent to claims management companies (CMCs) and fraudsters seeking to obtain high volumes of consumers' credit data. Making these requests free of charge, would be a charter for fraud and abuse. Although the proposal in the Regulation would enable the lender to charge for "manifestly excessive" requests, this may not prevent CMCs and fraudsters making identical requests across a large customer base.

19. The obligation to conduct a data protection impact assessment (Article 33) is overly bureaucratic and provides no added value given that the controller has to comply with the Regulation. Data processors cannot and should not be asked to make an assessment as to whether or not a legal obligation placed upon them poses a high degree of "specific risks." This is a consideration for the supervisory authority.

20. The employment of dedicated data protection officers (DPOs) (Article 35) will impose significant costs. Data specialists in the South-East of England can command salaries in excess of £75,000 pa. Because the current pool of data protection experts is very small, salaries would inevitably rise if DPOs became mandatory. The proposals are is likely to lead to a major increase in the data protection training market and spawn a new industry of data protection consultants (many of whom currently charge over £400 per day).

21. The DPO's tasks (Article 37) may make sense in the context of the operations of a large corporation. However, they are unrealistic for smaller organisations which may not need or be able to afford the services of such an expert. The core tasks of the data protection officer should be limited to monitoring on-going compliance.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

22. Yes they are. We strongly welcome the Ministry of Justice's pledge to challenge the European Commission's cost-benefit analysis. Many of our concerns have been recognized by the UK Government for example, the right to be forgotten, free subject access requests and the introduction of new bureaucratic requirements such as data protection impact assessments.

August 2012

Written evidence from the RSA Insurance Group

INQUIRY ON THE EUROPEAN UNION DATA PROTECTION FRAMEWORK PROPOSALS

EXECUTIVE SUMMARY

- RSA welcomes the opportunity to submit evidence to the Committee's inquiry on the EU Data Protection Framework Proposals.
- We support the new proposals being in the form of a Regulation rather than a Directive. As a multinational insurance group we welcome the European Commission's aim of creating a level playing field.
- We also support the administrative reduction that is to be included in the proposed Regulation, for example the simplification of notification filings; reduced requirement for transfer permits; Binding Corporate Rules formally recognised as an alternative transfer mechanism; and the concept of a single regulator for all EU processing.
- However, while these amendments go some way towards reducing the administrative burden for Data Controllers, there are other proposed amendments that would significantly increase the burden and which would outweigh the Commission's key aim of delivering an effective, pragmatic and standard Regulation across the EU.
- The need for proportionality is critical. The cost of implementing the new Regulation must not exceed the intended benefit.

— RSA welcomes the UK Government's approach and next steps, which incorporate our concerns as a Data Controller.

About RSA

1. RSA is a multinational insurance group writing business in 130 countries with major operations worldwide. We operate solely in the non-life insurance market. Across Europe RSA has businesses selling personal lines insurance, for example motor, home and pet insurance. RSA is also a major global commercial insurer, with particular expertise in large and risk managed businesses, marine, construction and engineering and renewable energy.

2. This submission is made on behalf of the RSA Group (www.rsagroup.com) and not in a personal capacity. As a business stakeholder, RSA is mainly interested in the Regulation for general and commercial data protection. Our submission is therefore focused on the Regulation and we do not comment on the Directive.

Q. *Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?*

3. 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, as currently drafted, the Regulation is not proportionate and there are a number of unintended consequences for businesses such as insurers.

4. One of these consequences is the ability by insurers to share information. While we support measures to ensure appropriate consumer protection, the changes will impact on the ability of insurers to share information to prevent fraud and other financial crime. It is vital that the legislative framework recognises the need for organisations to share information for such purposes, otherwise insurers will be restricted in reducing and deterring insurance fraud. This is an example of where insurers would be stifled by the regulatory burden placed upon them which in turn would not be in the overriding interests of society. For example:

(a) For *non-sensitive* data, Article 6 Clause 1(f) *"processing is necessary for the purposes of the legitimate interest pursued by the controller" may* be intended to include data sharing/processing for fraud purposes. RSA seeks confirmation that this provision will allow insurers to share data for this purpose; and

(b) As currently drafted the Regulation does not (outside of explicit consent) provide a right to process *sensitive* data. This is a concern to RSA and we believe a similar provision should be introduced for sensitive data. An exemption currently exists in UK Data Protection legislation for sensitive data (schedule 3 7A).

5. Another unintended consequence is our ability to access, process and store personal data, which is central to insurers' ability provide consumers with appropriate products at fair prices. Any rules on profiling should not prohibit or restrict risk-adequate ratings, rate classifications and risk assessments that are necessary for the purpose of premium calculation. There is a direct relationship between expected claims and the policy-holder's profiled risk. An assessment of these risks is the basis of technical insurance risk and adequate individual premium calculation. We are concerned that the inability to use data effectively would almost certainly result in consumer detriment in the form of higher prices and/or under insurance as it would inhibit the insurer's ability to weight according to risk. The Regulation should also allow for criminal convictions to be used for the purposes of insurance risk pricing.

6. RSA supports the administrative reduction that is to be included in the proposed Regulation, for example, the simplification of notification filings; reduced requirement for transfer permits; Binding Corporate Rules which will be formally recognised as an alternative transfer mechanism; and the concept of a single regulator for all EU processing. While these amendments go some way towards reducing the administrative burden for Data Controllers, there are other proposed amendments that would significantly increase the burden and which would outweigh the Commission's key aim of delivering an effective, pragmatic and standard Regulation across the EU.

7. One example is the change proposed with regard to breach notification. The proposals are disproportionate and will be unduly burdensome for businesses and Data Protection Authorities. We do not believe they will deliver the desired benefits for consumers. We propose that only breaches that pose a significant risk of harm to data subjects should be notified to the Data Protection Authority without undue delay. To do so within the 24 hour timeframe stipulated by the Regulation would be unrealistic. It should be noted that regulated financial services companies in the UK already have an obligation to notify those data security incidents to the FSA which may create a heightened risk of financial crime, or which affect the company's ability to provide adequate services to its customers.

8. Another example stems from the "right to be forgotten" provisions. Financial services firms are required to retain data to demonstrate regulatory compliance. RSA seeks confirmation that we can continue to do so when there is a legal/contractual or legitimate interest in place. Furthermore, the proposals place the burden of

proof on the Data Controller to provide evidence that explicit consent has been captured. It is unclear how this will dovetail with the right to be forgotten; if the consumer has the right to be forgotten and have all their data erased, how will the Data Controller be able to prove that consent has been legitimately captured if that too has to be erased. This would leave the Data Controller unable to defend any complaint relating to the capture of data.

9. Other measures which would increase the burden on Data Controllers include:

(a) Introducing the concept of Data Controller accountability will mean a significant increase in the level of paperwork required to evidence the processes and procedures required, for example, mandatory Privacy Impact Assessments; the adoption of Privacy by Design; maintaining security incident logs and the appointment of a mandatory and independent Data Protection Officer;

(b) General transparency requirements increased to include detailed Fair Processing/Privacy notices and a requirement to publish a Data Controllers' data protection policies;

(c) Responding to the exercising Data Subject rights; and

(d) Complying with data portability. The inclusion of an article on data portability is substantive but it clearly falls outside the scope of the legislation as it is not about data protection or security. The ability to change providers easily is a consumer and/or competition issue and should be dealt with under other relevant legislation at which point any data protection considerations can be taken into account.

10. Overall, we are concerned that too much focus on the granular can reduce data protection requirements into a tick box exercise for Data Protection Authorities and Data Controllers, rather than enabling them to focus their energy and resources on good data protection practices.

Q. *Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?*

11. Yes, we welcome the UK Government's approach and next steps, which incorporate our concerns as a Data Controller. In addition, the Government's proposals also seek to allow Data Protection Authorities and Data Controllers room to apply the requirements in an appropriate way.

August 2012

Written evidence from Equifax[1]

EXECUTIVE SUMMARY

— Equifax has serious concerns about the impact of the EU proposals;

— In particular the failure of the EU proposals to recognise the differences between critical "citizen" data and "consumer" data;

— We also believe that the current EU proposals could have a damaging impact on responsible lending levels, making it more difficult for consumers and businesses to obtain credit;

— The EU proposals could hinder the UK Government's drive to tackle instances of fraud, tax evasion and asset recovery;

— Consumers may also be impacted in their ability to access services, particularly those online services requiring identity verification; and

— While we are broadly happy with the general approach the UK Government is taking, we would like their reassurance that they will also raise concerns to the Commission to look at the specific apprehensions outlined below, especially those relating to data minimisation, profiling, legitimate interests, data portability and consent.

The role of credit reference agencies and the importance of financial data

1. We are grateful for the opportunity to submit evidence to the Committee's timely inquiry. An effective data protection framework is essential in order to protect an individual's right to privacy.

2. There is an understandable need to update the existing data protection framework, especially given how drastically the technology landscape has changed since the 1995 Data Protection Directive. However, in doing so great care must be taken to protect the integrity of critical data which form the basis for essential services accessed by Government, businesses and consumers.

3. At present we have some very serious concerns about the unintended consequences of the EU proposals. In particular the impact they will have on lending, access to data and the ability of Government to tackle instances of fraud.

[1] Equifax is a leading consumer credit reference agency, maintaining credit information on over 400 million individuals worldwide. We employ over 7,000 people in 16 countries throughout North America, Latin America, and Europe.

4. The primary responsibility of credit reference agencies is to facilitate qualified, informed assessments concerning the creditworthiness of individuals or commercial enterprises by offering historical credit data and other analytics to credit granters. The data held and managed by credit reference agencies such as ourselves is therefore a critical part of the UK's economic infrastructure.

Credit Reference Agency data is part of our critical national infrastructure

5. With regard to the Commission's data protection proposals, we believe there is an important distinction to be made between "citizen data"—the critical information necessary to make business, Government and the economy work- and "consumer data" such as a Facebook profile, twitter account or internet search history.

6. Among other functions, "citizen data" confirms an individuals' identity, where they live and their financial history. Citizen data is based on a range of sources including the electoral roll, utilities, telecoms, the banks and Government data. It empowers consumers to access services, and allows Government and businesses to make intelligent, responsible decisions. Examples of citizen data include a passport, credit reference file and driver's licence.

7. In the same way that public authorities need to independently verify an individual's identity, credit granters must be able to access reliable credit information in order to make responsible lending decisions. As such, we believe the distinction between critical "citizen data" and other types of personal data is an important one and that it is therefore imperative that data protection rules are flexible enough to take this into account.

The EU Data Protection Framework Proposals

8. Equifax welcomes an effective framework that protects data and individual rights in an efficient and robust manner. We consider the protection of personal data to be of paramount importance and we have stringent verification and data protection procedures in place to ensure that personal details stay secure.

9. However, we do not believe the European Commission's latest proposals strike the right balance between protecting an individual's rights and freedoms and the legitimate interests of commercial businesses.

10. In their current form, there is a significant risk that the proposals could restrict the ability of credit reference agencies to provide critical services to the financial services industry, Government and consumers. The detrimental impact of these changes would extend far beyond our business sector to the financial sector and the wider economy. On the high street, lenders will have less meaningful data on which to make lending decisions or to verify identify; the outcome becoming less lending and access to services, to consumers and businesses across the UK.

11. We are particularly concerned about the potential impact of the provisions for a "right to be forgotten"; this would restrict data controllers to only capturing the "minimum necessary" data, significantly reducing the quality of data provided to the Government, businesses and consumers.

12. The proposed articles concerning "profiling" could significantly restrict our business activities as our clients rely upon our regular scoring models to support responsible lending decisions all-year-round. The EU proposals would require consent needed to be given to profiling by an individual when signing a specific contract. This could result in credit scoring only being available for some purposes and only at certain times.

13. Furthermore, we are also concerned that proposals to give individuals the right to obtain copies of their credit data could be open to abuse by offering individuals the opportunity to edit their own credit history. The ultimate result of any measures which damage the integrity of credit data would be to negatively impact the availability of credit as lenders carrying out due diligence will be less likely advance funds.

14. We welcome the supportive role the UK Government is playing in putting these concerns forward, and we hope that it can work with the Commission to ensure that adequate protections are put in place to reflect the important role credit reference agencies play in the wider economy.

15. While we are broadly happy with the general approach the UK Government is taking, we would like their reassurance that they will also ask the Commission to look at the specific concerns outlined above and below, especially those relating to lawful processing, consent, data minimisation and profiling.

Issues with the Current Proposals

(A) *Data minimisation*

16. Article 5 (Principles Regarding the Processing of Personal Data) specifies that companies be only permitted to process, in a transparent manner, the minimum amount of data necessary to satisfy the purpose for which the processing was undertaken.

17. Notwithstanding the prevailing lack of clarity surrounding the qualifications to this Article (ie "not excessive" and "transparent"), these requirements appear to be inconsistent with the provisions of the Consumer Credit Directive, the "Mortgage Credit Directive", Anti-Money Laundering Regulations and Counter-Terrorism legislation, which mandate data accuracy and completeness in the interest of responsible lending.

(B) *The right to be forgotten*

18. The Right to be Forgotten and to Erasure proposed under Article 17 has serious ramifications for credit reference agencies. Allowing for the removal of the disputed data from credit files (pending resolution) would allow individuals to selectively edit their credit histories and negatively impact on the integrity of credit reference data.

19. Any reduction in the ability to verify an individual's identity and manage risk (particularly those associated with fraud) will have a detrimental impact upon credit reference services and a consequential effect of weakening credit decision-making processes. The ultimate result could have the potential to impact the availability of credit, as lenders carrying out due diligence will not advance funds where credit data is lacking or deficient. As such, this provision will not only have a detrimental impact upon responsible lending, but will materially affect the commercial interests of businesses in the financial sector.

(C) *Profiling*

20. Article 20 (Measures based on Profiling) provides that individuals have the right not to be subject to a process that extrapolates upon their characteristics based upon a pre-determined set of attributes.

21. Credit reference agencies utilise scoring models to support responsible lending and other legitimate activities. For example, Equifax's proprietary technology gives credit granters the ability to establish creditworthiness, an individual's ability to afford payments, and identify possible instances of fraud and money laundering, an area which the Government has shown an eagerness to tackle.

22. This provision could materially restrict, or even prohibit, such established and necessary practices, which are designed to support responsible lending and assist clients in satisfying their legal and regulatory obligations.

(D) *Legitimate interests*

23. Article 6 of the framework (Satisfaction of the Legitimate Interest) proposes that the processing of personal data should only be lawful to the extent that it is necessary to satisfy the legitimate interests pursued by the controller and provided that it does not also infringe upon the rights of the data subject in question.

24. In order to support responsible lending decisions, it is vital that credit reference agencies are able to share credit account performance history, which helps to ensure the correct businesses and consumers have access to finance.

25. Non-recognition of credit reporting as a legitimate interest would create substantial uncertainty around the acceptability of important services, and could potentially restrict, if not prohibit, companies from supporting responsible lending and satisfying their obligations under existing legislation, such as the Consumer Credit Directive, Anti-Money Laundering Regulations, and Counter-Terrorism legislation.

(E) *Consent*

26. Article 7 (Conditions for Consent) stipulates that data controllers must demonstrate that explicit, positive consent has been given. As drafted, this provision could be construed as suggesting that obtaining signed documentation is the only appropriate means of satisfying this requirement. It must be emphasised that consent may be obtained through other positive, explicit means, such as verbal or tacit consent.

27. Credit reference agencies obtain consent on a proxy basis. As such, significant time and investment would be required to satisfy the condition of "explicit consent" as well as establishing retrospective proof in circumstances where credit reference agencies are not in possession of the original consent.

28. The Regulation also appears to grant data subjects the authority to withdraw their consent, necessitating the erasure of relevant data. Again, this provision would contradict existing and proposed EU legislation requiring the retention of historical credit data and impact on the ability of credit granters to make informed lending decisions.

29. Finally, this Article also stipulates that consent shall not provide a legal basis for processing of personal data where there is a significant imbalance between the parties involved. Arguably, a significant imbalance is inherent to any transaction between an individual and a commercial business. As such, this Article could prevent such data from being utilised for the purposes outlined above.

(F) *Data portability*

30. Articles 15 and 18 propose that all individuals have the right to obtain copies of their data and/or have such data transferred to a third party. We are concerned that such arrangements could be open to abuse (through data alteration), negatively affecting data accuracy and veracity. The possibility that the recipient would have to discount or ignore the received data (given the increased need to mitigate against fraud) would be increased. Again this would have a negative impact on the responsible lending practices of credit granters.

31. The provision of data held within a bespoke database also entails considerable cost. Any "free of charge" access arrangements would cause entities to pass on administrative costs, which would ultimately be borne by the consumer.

32. Furthermore, the current (not for profit) contribution for data access is critical in deterring fraudsters from obtaining potential high volumes of credit data and account information and to discourage frivolous or vexatious requests aided, in particular, by claims management companies. Credit referencing agencies are unique in having a statutory obligation to provide data for a fee of £2, an affordable amount but one which acts as a deterrent to any vexatious requests. The fee also helps to ensure that security around the credit file remains incredibly high throughout the credit referencing process, this stringent security may be jeopardised under the EU proposals.

(G) *Breach notification*

33. Articles 31 and 32 would require data controllers to notify both their respective regulatory authority and the affected data subjects in the event of a personal data breach. In the UK, the Information Commissioner's Office has suggested that these provisions are too prescriptive.

34. We believe the proposed prior authorisation requirements and timescales for breach notification are unrealistic and counterproductive given the volume of data held by credit reference agencies and the variety of means by which this data can be accessed.

35. There is an additional need for clarification of what would precisely constitute a data breach (and the circumstances where such notification is then required). As the Information Commissioner's Office has previously indicated, current resource limitations would prevent them from dealing with both sets of requirements in an effective and timely manner.

36. In their current form, the provisions do not improve protection for consumers but merely add additional and unnecessary costly burdens upon controllers and, by extension, regulators. An element of proportionality and specific thresholds should therefore be introduced.

(H) *Fines*

37. The Regulation, through Article 79, introduces significantly higher penalties for procedural or record keeping breaches. While the Commission has appropriately articulated the conditions for each increment of penalty, it is inappropriate to conclude that the choice between levying a predetermined premium or a specific sum (based on turnover) should rest on a determination of operational size.

38. Fines should be a consequence of material failure rather than administrative deficiency. It would be inappropriate to penalise businesses for data processing with which they might not be directly associated or be directly at fault.

(I) *Delegated acts*

39. Article 86 (Exercise of the Delegation) provides the Commission with the authority to introduce subsequent and secondary provisions without due consultation and legislative process. The ability for the Commission to introduce new provisions without stakeholder consultation may actively run into conflict with its existing obligations under the Consumer Credit Directive, the proposed "Mortgage Credit Directive", Anti-Money Laundering Regulations, and Counter-Terrorism legislation.

40. Legislation concerning fundamental rights must be subject to parliamentary process that includes the consultation and input of experts and stakeholders in order to ensure its necessity, appropriateness, and effectiveness.

(J) *Supervisory regulator approval*

41. Article 34 (Prior Authorisation and Prior Consultation) would require all commercial entities to obtain approval from the relevant regulatory authority (eg the ICO) before the transfer of personal data to a country outside of the EU.

42. The provision of prior approval of the regulatory authority in each event or arrangement on international data transfer would severely restrict daily operations of credit reference agencies and those of their clients, as they would have to engage in costly and time-consuming processes in order to satisfy this requirement. Furthermore, this Article does not require the regulatory authority to respond within a prescribed timeframe.

(K) *Territorial scope*

43. Article 3 on Territorial Scope would mean that the Regulation would apply outside of the EU if a data controller that is based within the EU processes data outside this jurisdiction. It is our belief that this provision will conflict with existing regulatory provisions relating to credit reference agencies, and potentially also with the data protection legislation in the non-EU jurisdictions concerned.

44. Furthermore, the sensitivity of the data held by credit reference agencies necessitates the inclusion of appropriate data protection protocols and safeguards within contractual agreements with data processing centres outside of the EU.

Conclusion

45. In their current form, there is a significant risk that the proposals could restrict the ability of credit reference agencies to provide critical services to the financial services sector, consumers and government. The detrimental impact of these changes would extend far beyond Credit Reference Agencies to the financial sector and the wider economy.

46. We welcome the supportive role the UK Government is playing in putting these concerns forward, and we hope that it can work with the Commission to ensure that adequate protections are put in place to reflect the important role credit reference agencies play in the wider economy.

47. While we are broadly happy with the general approach the UK Government is taking, we would like their reassurance that they will also ask the Commission to look at the specific concerns outlined above, especially those relating to data minimisation, profiling, legitimate interests and consent.

August 2012

Written evidence from Professional Publishers Association

INQUIRY INTO EU DATA PROTECTION FRAMEWORK PROPOSALS

1. PPA and its Role

1.1 PPA is the trade body for UK magazine, journal and business media publishers. A full list of PPA members is available at: http://www.ppa.co.uk/cgi-bin/go.pl/ppamembers/index.html.

1.2 PPA's membership consists of some 200 publisher members and affiliates who publish consumer, customer and business magazines, journals, data and directories in addition to conducting research, organising conferences and exhibitions.

1.3 PPA members offer print, digital and online publications and services, including websites, apps, online and digital versions of print publications and publications and data only available online or through digital channels.

1.4 PPA members are significant contributors to the UK creative industries. The total value of the UK magazine and business media industry is estimated at over £4 billion,[2] with consumer magazines contributing around £2.5 billion[3] and business media (including magazines and directories) around £1.6 billion.[4] The UK magazine and journal industry directly employs 114,000 people.[5]

1.5 PPA understands and agrees with the Regulation's legitimate aim of increasing the protection of individuals' data. A lot has changed since the Data Protection Directive was passed in 1995. However, the Directive, with its principles based approach, has stood the test of time. PPA is concerned that a Regulation, which in contrast to the Regulation is prescriptive and will have direct effect in member states, has significantly widened the scope of data protection law and has gone too far in its aim of protecting personal data and risks disproportionately damaging businesses.

1.6 PPA's response will focus on the proposed Regulation for general and commercial data protection (the "Regulation") and not the proposed Directive covering processing in the areas of police and criminal justice.

2. Summary

2.1 The proposed Regulation does not strike the right balance between safeguarding the rights of individuals and allowing the development of innovative new products and services, including those that rely on advertising income (which enables digital content, services and applications to be made available to consumers at little or no cost).

2.2 PPA believe the proposals are burdensome, restrictive , potentially impracticable for UK advertising business models and likely to inhibit the flourishing of new digital services. The Regulation will likely have a significant negative impact upon digital business models as well as the businesses—many SMEs—that these support, as well as growth and innovation and the UK's status as the leading internet economy.

2.3 The proposals undermine innovative self-regulatory approaches—such as the EU self-regulatory programme for online behavioural or interest based advertising, explicitly supported by the UK Government—

[2] PriceWaterhouseCoopers Global Entertainment and Media Outlook: 201014 (please note that all figures have been converted from USD to GBP using the exchange rate as at 3 March 2011).

[3] Ibid.

[4] Ibid. The sector is therefore significantly larger than the UK recorded music market (around £1.4 billion) and the UK film industry (just over £3.5 billion).

[5] PPA analysis of the Periodicals and Journals Industry based on Annual Business Inquiry.

that seeks to meet the right balance and is built upon extensive consumer research into attitudes towards the internet, advertising and privacy.

2.4 The concept of "personal data" has been widened significantly in the Regulation and would place a disproportionate burden on businesses providing services that are beneficial to individuals—including those that use customisation to make content and advertising more relevant.

2.5 PPA has three main areas of concern over the Regulation. These cover the freedom to market; press freedoms; and barriers to business.

3. Freedom to Market

3.1 Publishers are an important channel for brands to market their goods and services to potential customers—and publishers also need to market their own goods and services, including printed magazine subscriptions and digital offerings.

3.2 The combined effect of the changes to the Directive proposed in the Regulation is that it is going to become much more difficult and costly for businesses to market their goods and services to potential customers, without necessarily providing any increased protection for individuals.

3.3 The revised definition of "the data subject's consent" so that in all cases such consent must be explicit is problematic. It does not take account of the various ways that personal data may be obtained in a transparent manner—and with clear consent—that would be lawful under the Directive, but may not satisfy a strict interpretation of explicit. Such an approach does not take into account of the way data is captured in reality, particularly in relation to digital. There is a risk, for example, of publishers having to include tick boxes to the detriment of user experience when collecting data online, when consent could be gained clearly and transparently without an "explicit indication".

3.4 A more nuanced approach is required to consent. It will not always be desirable or practical—from both a consumer and publisher perspective—to require explicit consent.

3.5 PPA welcomes recognition in the Regulation that data controllers, such as publishers, may continue to process personal data where they have a "legitimate interest" (Art 6(1)(f)) without necessarily having gained prior consent, subject to a data subject having the right to object to such processing (Art 19).

3.6 However, uncertainty is created by the removal in the Regulation of the wording "or by the third party or third parties to whom the data are disclosed" which was included in the Directive. That wording provided that personal data may be processed where necessary for the legitimate interests of the data controller or third parties to whom data is disclosed. Does the revised wording in the Regulation mean that when publishers provide personal data to subscription fulfillment houses to distribute their magazines that the subscription houses would be in breach of the Regulation? Or would it mean that a publisher could not process personal data passed to it for bona fide purposes by a data controller without breaching the Regulation—for example an employer (the controller) signing up certain employees to receive a controlled circulation printed business magazine applicable to the employers' industry at the business address? Would a publisher not be able to fulfill such a legitimate request—or even seek the employees' consent—without breaching the Regulation as the legitimate interest of the employer (the controller) does not extend to the publisher (the third party to whom the data is disclosed)?

3.7 Direct marketing of press subscriptions is critical to safeguarding press distribution and routes to market. In 2009, 17% of the UK magazine market was based upon subscription and it is expected that this number will continue to rise.[6] The change to Art 6(1)(f) would likely negatively impact on subscription sales as a result of the negative impact on direct marketing of such subscriptions.

3.8 Furthermore, there is a danger to the controlled circulation business and special interest magazines which are sent to relevant professionals (doctors, lawyers, dentists, architects etc) without the recipients' prior consent (such as in circumstances highlighted above).

3.9 The wording covering third parties highlighted above was clearly inserted in the Directive for a reason—and its deletion in the Regulation creates uncertainty and potential problems for publishers. It is important that Art 6(1)(f) is maintained, and the wording "or by the third party or third parties to whom the data are disclosed" reinserted in line with the Directive. Such wording is even more important due to the direct applicability of the Regulation and the inability of the UK government to provide such nuance in implementing legislation.

4. Press Freedom

4.1 The Regulation is far more onerous for data Controllers than the Directive. This is expanded on below. Journalists and publishers benefit from certain exceptions under the Directive (Art 9), and in the UK under s.32 of the Data Protection Act 1998 that enable them to perform their journalistic function and produce professional and authoritative content.

[6] Audit Bureau of Circulation actively purchased copies.

4.2 A publisher, as a data controller, may process personal data as part of the publication of journalistic material if it reasonably believes that publication is in the public interest—in order to protect freedom of expression.

4.3 These exceptions allow publishers to research material for articles, day to day newsgathering, investigation, and editing. And it also enables publishers to publish personal data in their publications, including online (which remain online as archives, searchable by future generations).

4.4 Such exceptions to processing personal data are vital for publishers and investigative journalists to be able to continue to do their jobs. The exceptions are finely balanced and it is important that they are maintained.

4.5 However, the implications of the Regulation are unclear. Unlike the vast majority of the Regulation which is prescriptive, exceptions for journalistic purposes and freedom of expression are carved out and left for individual member states to address. Harmonization of data protection as it applies to individuals, including the right to be forgotten, is set out in the Regulation whereas the protection for publishers will be piecemeal (and likely to change on a country by country basis). As such, there must be a danger that publishers that print accurate stories about individuals that are in the public interest, but those individuals do not necessarily like what is written, will lead to such individuals challenging publishers and demanding that material is taken down under the right to be forgotten.

4.6 In such circumstances, with the journalistic exceptions not harmonized, what would happen with regard to cross border complaints about online material? Which countries' laws would apply if a Hungarian citizen complained about an online article published by a UK based publisher and requested that it is taken off the publishers' website in accordance with the right to be forgotten? What would happen if the Hungarian law did not provide appropriate safeguards for journalistic purposes: could a Hungarian citizen obtain an injunction under such a Hungarian law to have such content removed as the Regulation does not address journalistic exceptions?

4.7 The "right to be forgotten" poses real dangers for the press. This ill defined concept could lead to publishers being forced to remove legitimately published information about an individual because an individual does not like what was written. As well as the practical problem of magazine publishers being forced to remove content from its site, the historical record that publishers provide could be jeopardised. An analogy would be an individual having the right to force the British Library to physically remove articles from its digital and paper based archives (such as legal deposit material) under the right to be forgotten—because in the present and future publishers websites serve and will serve as a historical archive. Such a historical archive should not be threatened.

4.8 Journalism, publishing and freedom of expression need to be carefully considered and appropriate safeguards provided for.

5. Barriers to Business

5.1 It is important that businesses are not unnecessarily burdened with "red tape" that does not actually provide any meaningful or additional protection for individuals. Magazines are an important part of the press—both in print and digital—and the press should not be threatened by burdensome restrictions that do not serve their aim of protecting individuals' data.

5.2 The definitions of "data subject" and "personal data" significantly widen the scope of data protection legislation. Under the Regulation, data that may not actually identify a living individual could still constitute personal data and as such be subject to the Regulation (and eg subject access requests, access to data, the right to be forgotten etc). This is likely to lead to practical problems and additional costs for businesses. How is a publisher that receives a subject access request to fully respond when much of the "personal data" it may have could have to be married with other data before it is clear to which living individual it relates? This will take time, effort and money—but will it provide additional protection? If data cannot identify an individual without further investigation, should that be subject to all of the Regulation? Perhaps there needs to be a more nuanced approach to different levels of personal data to avoid practical problems.

5.3 Furthermore, the Regulation is going to take a lot of negotiation before it is finalised; but once it is entered into the EU's Official Journal, the Commission will be able to make potentially significant changes to the Regulation using "delegated acts in accordance with Article 86". This appears to be a "Henry VIII" clause that could be used to adapt then Regulation relatively easily without proper scrutiny—and such changes would be applicable in all member states. PPA is concerned that potentially damaging changes could be made to the Regulation without the proper democratic scrutiny that is clearly advisable—especially as the Regulation provides for such large fines for breaches.

August 2012

Written evidence from Christopher Millard, Alan Cunningham and Kuan Hon, Cloud Legal Project

EU DATA PROTECTION FRAMEWORK PROPOSALS

1. This response is by Christopher Millard, Alan Cunningham and Kuan Hon, Cloud Legal Project (**CLP**)[7] http://cloudlegalproject.org**,** Centre for Commercial Law Studies, Queen Mary, University of London.[8] We have researched cloud computing since 2009. The Annex describes cloud computing and our research's scope.

2. Cloud computing's potential importance is recognised.[9] Data protection laws considerably affect cloud computing. This response, based on our research, addresses the proposals' impact on cloud computing from both service providers' and users' perspectives (but not how they might affect Queen Mary, University of London as an institution, ourselves as individuals using cloud computing in professional or personal capacities, or any specific body of users or providers).

3. SUMMARY

— Overall, we welcome the intention to clarify and modernise data protection rules.

— Our comments aim to minimise unnecessary regulatory burdens, complexity and uncertainty for the developing cloud industry and, indeed, burdens—whether direct or passed on via cost or other means—for potential cloud users.

— We understand prospective cloud users must comply with data protection laws, but believe there are more effective (and less burdensome) ways of encouraging industry development while addressing user concerns, such as raising awareness of secure encryption options, and fostering and supporting parallel development of industry standards and certification systems regarding data privacy and security. We therefore welcome proposals in these areas (including privacy by design and privacy by default) as a positive attempt to encourage best industry practice, which could help promote trust amongst actual and potential users. However, further clarification and guidance on those provisions is needed.

— The table below compares key issues under the current regime and the proposals. We believe they are crucial both for the cloud sector and cloud users, and need addressing.

Issue	*Data Protection Directive*	*Proposals*
1. Scope of "personal data"	Existing laws only apply to "personal data". Currently, much data in the cloud are considered "personal data", whatever the practical likelihood of identification or risk or likely extent of harm. This creates unnecessary burdens for many providers.	The proposals would not reduce the likelihood of much cloud data being considered "personal data" under data protection law. If anything, they may increase it, further increasing burdens on providers.
2. Nature of cloud services	Existing laws treat providers as either data processor or data controller (or both). But infrastructure providers with little or no knowledge of, or control over, use of personal data, may essentially be neither, but merely passive intermediaries.	The "either processor or controller (or both)" model is maintained. A more nuanced definition of "processor", or exemption for providers acting as passive intermediaries, would be welcomed.
3. Determining jurisdictional matters	Existing laws do not adequately reflect many cloud arrangements' logistics, determining jurisdiction based on "establishment" of the controller or use of equipment in the EEA. This may discourage establishment and/or use of EEA-based cloud infrastructure or services.	Non-EEA providers and users may still become subject to data protection rules simply through using an EEA data centre or provider. While we welcome the proposed "offering goods or services" test, further clarification is required on the derogation's scope.
4. International transfers of personal data outside the EU	Existing laws focus unduly on data location, rather than restricting unauthorised access to intelligible data.	Additional restrictions on transferring personal data to third countries. A new derogation—for transfers not "frequent or massive", necessary for the legitimate interests of the controller or processor—is welcome. However, the "frequent or massive" concept is unclear, and seems unnecessary.

[7] The CLP team comprises: Prof. Christopher Millard, Prof. Chris Reed, Prof. Ian Walden, Dr. Julia Hörnle, Dr. Alan Cunningham, W Kuan Hon and Simon Bradshaw.

[8] The Cloud Legal Project was made possible as a result of generous charitable donations from Microsoft Corporation. These views, however, are the independent views of the research team.

[9] Commissioner Kroes has expressed the desire to "remove obstacles—and indeed give a boost—to a competitive and effective cloud market". Neelie Kroes, EU Data protection reform and Cloud Computing, Microsoft Executive Briefing Centre Brussels, 30 January 2012.

Issue	*Data Protection Directive*	*Proposals*
5. Law enforcement access to data in cloud environments	Existing laws may render disclosure to non-EEA law enforcement agencies unlawful, creating much legal uncertainty for users and providers.	Existing uncertainties are perpetuated. Clarification would be welcomed.
6. New issue for cloud: Increased bureaucracy and compliance burdens		New requirements on data protection impact assessments, consultation with regulators, data protection officers and detailed documentation.
7. New issue: Increased role of supervisory authorities		Increased regulatory oversight. While there is a clear case for improving transparency, security and accountability, providers who are mere intermediaries may be subject to inappropriate regulation.

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

4. *Overview.* In cloud computing, we consider the proposals would not strike the right balance between effective data protection and regulatory, financial and administrative burdens. Indeed, they may increase burdens without necessarily improving data protection, because the proposals would not resolve certain existing problems (outlined further below), but would compound some of them.

5. *"Personal data"*. The proposals would not clarify sufficiently the "personal data" definition, which is the trigger for applying EU data protection laws. Currently, much cloud data are "personal data", to which the regime applies irrespective of availability of secure encryption, practical likelihood of identification, or risk or likely extent of harm. This is an unnecessary regulatory burden, particularly on providers. We believe alternative tests of likelihood of identification/risk and likely extent of harm would better reflect technological and logistical realities of cloud business/technology models and use. Also, the proposals should address specifically the role of encryption and the status of encryption or anonymisation processes and encrypted data.

6. *Nature of cloud services*. Currently certain providers, who may merely provide infrastructure services (facilities and/or tools) to be used autonomously by end-users or intermediate platform or service providers ("infrastructure providers"), are nevertheless subject to data protection rules. Instead of recognising the nature, complexities and nuances of cloud services, the proposals would perpetuate the binary "controller"/"processor" distinction and impose new obligations and liabilities on "processors", such as requirements regarding provisions in controllers' contracts with processors, many of which ill suit cloud services models.[10] This may obstruct development of multi-layered cloud services, particularly for market entrants wishing to establish data protection-compliant services using third party platforms or infrastructure, which may reduce users' market choice. We recommend a more nuanced definition of "processor", and/or modernising and extending E-Commerce Directive exemptions to cloud services whose providers are merely passive intermediaries, and who should therefore benefit from that Directive's intermediary immunities (unless and until acquiring the requisite knowledge and control regarding personal data processed by customers using their resources). Development and legal recognition of suitable industry standards and certifications could help address concerns regarding providers and sub-providers.

7. *Jurisdictional matters*. While we welcome proposals to abolish "means"/"equipment" tests and base data protection jurisdiction on targeting, we consider that, for legal certainty, the meaning and scope of the proposed terms and definitions need clarification, particularly "offering", "only occasionally", "monitoring" and "main establishment". The concept of "directing" is better understood than "offering". Currently, providers and users risk becoming subject to data protection rules if they use an EEA data center or EEA provider, without sufficient clarity as to which Member State's regulator has authority over them. This may disincentivise non-EEA users from using EEA providers or data centers. The proposals would perpetuate and indeed exacerbate these problems, given proposed extensions of data protection regulation to personal data processing in the context of activities of a *processor's* EEA establishment, without exemptions for cloud intermediaries. Finally, the proposals would not close a loophole, discussed in our research,[11] which may undermine protection for some EU residents when using services of non-EEA providers.

8. *International transfers of personal data outside the EU*. Given the ease of remote access and data transfers in the internet age, we consider that security, accountability and transparency are more important, in terms of effective privacy, than data location. We argue the focus should be on restricting unauthorised access to intelligible data, rather than restricting international data transfer *as such*. For example, where data are securely protected via strong encryption, focusing primarily on their geographical location may be unnecessary and may restrict inappropriately use of cloud services. Ease of data transfer to third countries can facilitate considerably

[10] See table in Annex.
[11] Annex, 2.4.

development and efficient use of cloud services. The proposals would, rather than making data location simply one element affecting security, impose additional restrictions regarding transfer of personal data to third countries, including requiring regulatory approval. This would increase regulatory burdens on EU businesses using cloud services involving personal data transfers to third countries, compounding current difficulties. A proposed derogation for transfers to a third country necessary for "the purposes of the legitimate interests pursued by the controller or the processor" might be helpful, but would not apply to transfers that are "frequent or massive", and thus would not assist cloud computing. We argue the focus should be on appropriate safeguards, rather than size or frequency of transfers. Legal recognition of appropriate industry standards and certifications could allow security to be maintained while allowing international transfers.

9. *Law enforcement access to data in cloud environments*. Uncertainty regarding law enforcement access to data in cloud environments may discourage cloud adoption. Current laws permit processing for law enforcement purposes, and exempt certain processing from some data protection obligations where necessary for reasons including "the prevention, investigation, detection and prosecution of criminal offences". However, where an EEA provider responds to a request for personal data from a *non*-EEA law enforcement agency, transfer of data outside the EEA must be legitimate under data protection rules. Absent "adequacy", the Directive's Article 26 offers certain exemptions, but the relevant exemption's scope is also uncertain. Current laws may, therefore, render disclosure to non-EEA law enforcement agencies unlawful. The resulting legal uncertainties for users and providers could deter take-up of cloud services.

10. *Increased bureaucracy and compliance burdens*. The proposals are likely to increase bureaucracy and compliance burdens for controllers and processors. As infrastructure providers are likely to be considered "processors"—while being, in reality, merely passive intermediaries—we believe these expanded responsibilities would be inappropriate; for example, impact assessments, and new record keeping responsibilities. While there is a clear case for promoting accountability, security and transparency in the cloud, greater flexibility may be required to facilitate cloud services development and accommodate industry standards, especially for those infrastructure providers we believe should be considered neither controller nor processor.

11. *Increased role of supervisory authorities*. The proposals expand data protection supervisory authorities' role. For example, the national supervisory authority of the country that is the "main establishment" of a cloud provider would be competent to supervise its processing activities in all Member States (proposed Article 51). Furthermore, controllers and processors must consult and seek authorisations from national supervisory authorities for certain personal data processing, for example many data transfers to third countries (proposed Article 34). Again, we welcome initiatives to promote a cloud environment where transparency, security and accountability are the norm. We are concerned, however, that infrastructure providers will also be unnecessarily subject to this increased regulatory oversight. Clarification here would be welcome.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

12. The Summary's "next steps" are at a high level. We support the proposal to resist new bureaucratic and potentially costly burdens on organisations which do not appear to offer greater protection for individuals, if it addresses the cloud issues outlined above at a detailed level.

August 2012

Annex

1. Cloud Computing—Definition and Differences

The CLP definition is:

- Cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in relation to demand.
- Services (especially infrastructure) are abstracted and typically virtualized, generally being allocated from a pool shared as a fungible resource with other customers.
- Charging, where present, is commonly on an access basis, often in proportion to resources used.

Cloud service models[12] are often categorised as Infrastructure as a Service ("IaaS") (providing computing resources like processing power and/or data storage), Platform as a Service ("PaaS") (providing tools for developing and deploying custom applications, eg certain mobile applications), or Software as a Service ("SaaS") (providing end user applications, like webmail or online word processing).

Current laws, and the proposals, envisage traditional outsourcing and stand-alone databases (in use when current laws were drafted). They do not cater adequately for key differences arising from service type, particularly with public shared-infrastructure IaaS and PaaS (ie infrastructure services), or differences arising from individual services' designs:

[12] Mell and Grance, The NIST Definition of Cloud Computing (2011).

Traditional assumptions	*Cloud computing*
1.1 Active agent, vs self-service usage	
Traditional outsourcing: controller hires processor, who actively processes data for controller according to controller's instructions.	Controller rents IT resources from provider. Controller processes data in self-service fashion, using infrastructure/resources supplied by the provider—as when renting computers. Many infrastructure providers do *not* actively act as agent processing data for controller, but at most passively store data the controller has chosen to store on the provider's infrastructure. Current requirements for providers to follow controllers' "instructions" in processing data make little sense with infrastructure services where the *controller*—not provider—processes data, using the provider's resources. Providers maintain standardised infrastructure and environments for users' data processing. If users can specify setup of shared infrastructure (eg security-related measures), this undermines the cost-saving commodity characteristic of cloud; also, it may be impossible for providers to comply if different users' instructions conflict. The underlying concerns are that providers or others could (1) access intelligible data, or (2) undermine data integrity. On (1), see 3. below. On (2), controllers may backup internally or to other cloud services. On both, certifying services' security to minimum industry standards seems more workable for facilitating risk assessments than "instructions" requirements, particularly as many users lack technical expertise.
1.2 "Direction of travel" and sequence of events	
Controller hires processor to meet controller's specific processing needs. Processor may engage sub-processors to assist with its processing duties.	Provider offers pre-packaged commoditised services (sometimes built atop third party services, usually on the third party's standard terms). Controller chooses the provider and pre-built package for its specific processing and other needs. Customisation is sometimes possible, but costs extra time/money.
1.3 Data location and data deletion, vs access to intelligible data	
With stand-alone databases, eg on tape drives, where data are unencrypted or insecurely encrypted, whoever physically holds the media may access stored data upon knowing the file format (to interpret the 1's and 0's). Media location therefore affects security.	Given distributed storage and proprietary file formats, access to physical media, eg storage hardware in a third country, does not necessarily afford access to intelligible data. The only sure way to access intelligible data is through the user logging in to reunite fragments into intelligible form automatically. Fragments are distributed automatically; providers may or may not know in which hardware all fragments comprising one data set are stored. Some fragments may be intelligible, others not. Some providers can bypass or use customer logins, others cannot. Even providers bypassing customer logins cannot, without decryption keys, decipher data securely encrypted by controllers. Similarly, after deletion operations, fragments may or may not be intelligible or re-unitable. Again, these depend on service type and design.
1.4 User control	
Controller closely controls processing.	Cloud services differ. Users do not necessarily lose all control in the cloud; they may encrypt data, IaaS users may install firewalls, system design may affect what's controllable. Regulating all cloud services alike, as if they posed equal risks to privacy, could impede cloud development and use.
1.5 Security	
Controller dictates security requirements.	See 1.1. Some regulators acknowledge that too much disclosure about shared infrastructure may undermine security.

2. CLP Research to Date on the Following Legal Implications of Cloud Computing

2.1 Standard contract terms[13]—surveyed 31 standard contractual terms and conditions of US and European cloud providers.

2.2 Negotiations of changes to standard terms[14]—based mainly on detailed interviews with UK and global cloud providers, customers and others.

[13] Bradshaw, Millard, and Walden, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services (2010) http://ssrn.com/abstract=1662374.

[14] Hon, Millard, and Walden, Negotiating Cloud Contracts—Looking at Clouds from Both Sides Now (2012) http://ssrn.com/abstract=2055199

2.3 UK G-Cloud v1 and cloud contracts.[15]

2.4 Determining data protection jurisdiction.[16]

2.5 Scope of "personal data".[17]

2.6 Nature of cloud service under data protection laws.[18]

2.7 International data transfers in the cloud under data protection laws.[19]

2.8 Information ownership.[20]

2.9 Competition law issues.[21]

2.10 Law enforcement access to cloud data.[22]

Written evidence from the United States Chamber of Commerce

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses and organization of every size, sector, and region, including many members that are representative of a vital transatlantic business community that is essential to increasing jobs and growth on both sides of the Atlantic. We support the development of clear, consistent data privacy regimes that protect consumers, while promoting innovation through the unimpeded flow of data for legitimate uses. The Chamber applauds the proactive approach to stakeholder engagement taken by the UK Government regarding the recent EU data protection proposal. We look forward to working with the UK to develop a final Proposal that assures the protection of the public's privacy through the enhancement of the European Union's data privacy regime in a manner that is efficient, flexible, practical, and allows for the continued innovative development that maintains and grows benefits to consumer, regulators, and businesses alike.

In response to the call for evidence.

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

The proposed Regulation fails to strike the right balance. Many of the proposed protections are not practical and will have unintended consequences that may actually serve to remove or restrict benefits currently in place while only adding confusion and burdens without additional protections. Moreover, the overly prescriptive nature of the proposal will greatly stifle business. For example, the proposed Regulation is too rigid in requirements on the way companies process personal data, assess risk internally, and respond to access requests in every sector. Sections on the "Right to be Forgotten" and "Data Portability" are also confusing and often unworkable across all business sectors, especially products and services that are already highly regulated. Prescriptive rules surrounding "Subject Access Requests" may actually put consumers at risk of identity theft. Recent studies estimate that within the next ten years products and services using the free flow of data will add over $1 trillion of annual value to consumer, business, and government end users in the U.S. and EU and we must avoid unnecessary regulatory burdens, like those found in the proposed Regulation to best to realize these gains.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

The general approach taken by the UK Government appears to be on the right track. We support the strategy to negotiate at EU level for an instrument that does not overburden business, the public sector or other organisations, and that encourages economic growth and innovation. We would emphasize two key points that would obviate many of the potential problems of the proposal and therefore should be broadly applied to all the bulletpointed next steps in the Summary of responses. First, the UK government should focus on developing a proposal that allows for flexible solutions that consider both the nature and purpose of the data being collected. Second, we would suggest encouraging solutions that maximize interoperability and allow for compliance with any domestic and international requirements that conflict with the current proposal.

---

[15] Hon, Millard, and Walden, UK G-Cloud v1 and the Impact on Cloud Contracts (2012) http://ssrn.com/abstract=2038557

[16] Hon, Hörnle, and Millard, Data Protection Jurisdiction and Cloud Computing—When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3 (2012) http://ssrn.com/abstract=1924240.

[17] Hon, Millard, and Walden, The Problem of "Personal Data" in Cloud Computing—What Information is Regulated? The Cloud of Unknowing, Part 1 (2011) http://ssrn.com/abstract=1783577

[18] Hon, Millard, and Walden, Who is Responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Part 2 (2011) http://ssrn.com/abstract=1794130

[19] Hon and Millard, Data Export in Cloud Computing—How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4 (2011) http://ssrn.com/abstract=1925066

[20] Reed, Information "Ownership" in the Cloud (2010) http://ssrn.com/abstract=1562461.

[21] Walden and Luciano, Ensuring Competition in the Clouds: The Role of Competition Law? (2011) http://ssrn.com/abstract=1840547

[22] Walden, Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent (2011) http://ssrn.com/abstract=1781067

Regarding specific comments on the next steps from the Call for Evidence:

— *resist new bureaucratic and potentially costly burdens on organisations which do not appear to offer greater protection for individuals; examples of this include mandatory data protection impact assessments, seeking prior authorisation from the supervisory authority for certain processing operations and the mandatory designation of independent data protection officers.*

We suggest adding a reference to data portability and wish to highlight that some of the burdens are not just costly, but also overly prescriptive and would effectively render certain business sectors inoperable under current legal and technical requirements. An opportunity also exists for the Regulation to incentivize companies that are already investing and continue to invest in data security, recognizing companies implementing policies, procedures, and standards consistent with industry best practices for securing personal data in computer systems and databases, by allowing them to process personal data freely across country borders:

— *support the introduction of data breach notifications both to supervisory authorities and affected individuals, but only if the provisions reflect the timescales needed to properly investigate a breach and if a sensible and proportionate threshold is provided which excludes minor and trivial breaches from the scope of the requirement.*

We suggest changing "excludes minor and trivial breaches" to "is limited to situations where harm presents a significant risk" to add clarity:

— *reaffirm its commitment to a strong and independent supervisory authority at national level and support the establishment of a consistency mechanism to ensure a degree of harmonisation in the application of data protection rules across the EU, whilst allowing independent national authorities some flexibility in how they use their powers.*

In regards to strategy on the role of Data Protection Authorities (DPAs), we suggest seeking clarification as to the extraterritorial reach of DPAs, establishing exemptions for businesses that do not have a physical presence in the EU and do not purposefully avail themselves to EU residents, and also seeking clarity as to how different Member State DPAs would interact when functioning as "one-stop shops":

— *support a system of administrative penalties for serious breaches of the Regulation's requirements, but push for a more proportionate level of maximum fines, which allows supervisory authorities greater discretion in applying the powers available to them.*

We suggest avoiding any result that ties penalties to a specific percentage of "annual worldwide turnover" as this presents additional definition and accounting problems and, in the rare event clarity could even be achieved, would represent an arbitrary and unpredictable (due to possible yearly and monthly fluctuations on "turnover") penalty amount.

In order to realize the many important goals undergirding the Regulation, the final version must allow for a flexible approach to privacy, avoiding a one-size-fits all approach that would impose unnecessary restrictions and costs without affording additional protections to consumers. An optimal result will ensure clarity and interoperability of different data privacy regimes. Any changes to existing requirements should also emphasize consistent and predictable enforcement across all member states. In particular, special attention should be paid to allowing for innovation and accounting for future developing technology. We thank you for considering our comments and we look forward to working with you to create an optimal solution.

August 2012

Written evidence from the Wellcome Trust

EU DATA PROTECTION FRAMEWORK PROPOSALS

Key Points

— The Government must make the protection of research one of their priorities in negotiations on the Regulation.

— It is essential that Article 83 and associated derogations are maintained as the Regulation moves through the legislative process. Amendments to clarify and strengthen the research provisions would be beneficial to ensure these achieve their intended purpose and do not inhibit important health research.

— Amendments are needed to ensure that the use of pseudonymised data in health research is regulated proportionately and to ensure clarity in the scope of the Regulation.

Introduction

1. We welcome the opportunity to respond to this inquiry since it is vital that the EU and UK can establish a regulatory framework that balances the rights and interests of individuals with the societal benefits of research using patient information. Our response focuses on the aspects of the proposed Regulation that affect health research. We are also submitting a joint statement from the Trust and other health research organisations that was presented to the Ministry of Justice during their call for evidence. This statement sets out the impacts of the data protection proposals for the sector and includes a number of case studies.

2. Information from patient records provides the foundation for much health research, and offers significant potential to answer questions about the factors that influence health and disease. Information from patient records can be used for epidemiological research; to understand more about the causes of disease; to detect outbreaks of infectious diseases; to monitor the safety and efficacy of drugs and medical devices; and to study the effectiveness of treatments and interventions. Patient information is also used to identify participants for research studies. Researchers may wish to approach individuals in order to gain their consent to participating in a particular piece of research, for example the trial of a new treatment for a particular disease.

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

Research derogations

3. The Regulation provides a number of derogations from particular requirements for the use of "personal data" for scientific research, providing that personal data is processed in accordance with the conditions set out in Article 83. These derogations do not exempt research studies from all the requirements set out in the Regulation. The Wellcome Trust warmly welcomes this approach since it provides a framework that balances the facilitation of research with the protection of the interests of research participants. However, to safeguard this balance the Government must prioritise the protection of Article 83 and ensure the associated derogations for research are protected as the Regulation moves through the legislative process.

4. There are a number of issues around Article 83 and the associated derogations that would benefit from clarification to better reflect the intent of the clauses. The lack of clarity in the current UK Data Protection Act has contributed to a risk-averse culture among those sharing and using data for research, which has led to delays to important research.

5. In order to avoid replicating these difficulties, it is essential that any lack of clarity is rectified in the new Regulation. The following clarifications are needed:

- Clarification of Article 6.4 and Recital 40 to ensure that the processing of personal data for other purposes intends scientific research to be viewed as a compatible purpose in itself.
- Clarification that the reference to Article 83 (processing for historical, statistical and scientific research purposes) within Article 81 (processing of personal data concerning health) is intended to link the two sections, rather than to impose an additional restriction on research.

6. A number of aspects of the research requirements and derogations rely on demonstrating "necessity".[23] While this approach is reasonable in principle, it will be important that an appropriate and consistent definition of "necessity" can be applied in this context to ensure clarity and proportionality in implementation.

Scope of the Regulation

7. The scope of the Regulation is "personal data" that identifies a natural person, or from which a natural person can be identified.[24] It is important that the research community is clear about when the different types of data used in research—anonymised data; key-coded or pseudonymised data; and identifiable data (see Annex A)—are considered to be "personal data". This determines whether a research study is brought within the remit of the Data Protection Act and therefore must comply with its requirements. Clarity in the scope is essential so that those sharing and using patient data in research are fully aware of their responsibilities, but do not impose unnecessary additional requirements that will stifle research.

8. The Regulation is not explicit on whether pseudonymised data are intended to be included within its scope. Pseudonymised or key-coded data underpin a substantial amount of research, for example studies at the Wellcome Trust Sanger Institute and the UK Biobank research resource. In the UK, the Information Commissioner has published draft guidance[25] to the effect that pseudonymised data can be considered anonymous—where identification does not take place, or where identification does take place and the data protection principles are not breached—and therefore falls outside the scope of the Data Protection Act. Inclusion of pseudonymised data within the scope of the Regulation would therefore dramatically increase the regulatory burden on research.

9. The use of pseudonymised data in health research is well-established and operates within a system designed to reduce the possibility of re-identification of participants. It is important that the use of pseudonymised data in research is handled within a proportionate regulatory framework that takes into account the actual likelihood of re-identification under current conditions, not just the technical possibility of re-identification. Conditions that will reduce the actual likelihood of re-identification could include the use of "safe havens", such as England's new Clinical Practice Research Datalink and comparable services in the devolved nations; contractual data sharing agreements; and professional standards for researchers that prohibit re-identification. In many instances the identifying code will not be held at the research site where the pseudonymised data are used in research, but at a hospital or by a safe haven. The Regulation should be

[23] For example Articles 6.2; 9.29(i); 17.3(c); 83.1(a); and 83.2(c).
[24] Articles 3 and 4.
[25] http://www.ico.gov.uk/about_us/consultations/our_consultations.aspx

amended to provide greater clarity on this issue for research, for example by noting that conditions could be established in a Member State that preclude re-identification, therefore ensuring that re-identification would not be considered "reasonably likely". The UK Government must ensure that the proposed Regulation does not increase the regulatory burden of using pseudonymised data in research.

10. Anonymous data falls outside of the scope of the Regulation. However, the act of removing identifiers to ensure that data are no longer personal—anonymisation—could fall within the definition of processing (Article 4). This would mean that the process of anonymisation itself would have to comply with the requirements of the Regulation to be lawful. We suggest that the Regulation should be revised to expressly permit anonymisation, while prohibiting re-identification for data that has been anonymised.

11. Clarification is needed around "genetic data" and "data concerning health" to ensure that these definitions are only intended to apply to personal data that falls within these categories, rather than all related data. Further, the definition of "data concerning health" should be clarified and must be consistent with Recital 26 to make it clear that data concerning health does not include biological samples *per se*, but rather to personal data obtained from testing such material.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

12. The Government's *Summary of Responses* to the Call for Evidence recognises the issues for research in the draft Regulation (pp31–32). However, research is not reflected as a priority in the Government's proposed next steps. It is important that this is rectified to ensure that the draft Regulation does not hinder research in the public interest. Particular steps the UK Government must take to protect the balance between the rights and interests of individuals and the societal benefits of research using patient information, include:

- Protecting Article 83 and the associated derogations for research as the Regulation moves through the legislative process.
- Seeking amendments to clarify and strengthen the research provisions to ensure these achieve their intended purpose and do not inhibit important health research.
- Ensuring that the proposed Regulation does not increase the regulatory burden of using pseudonymised data in research.

The Wellcome Trust is a global charitable foundation dedicated to achieving extraordinary improvements in human and animal health. We support the brightest minds in biomedical research and the medical humanities. Our breadth of support includes public engagement, education and the application of research to improve health. We are independent of both political and commercial interests.

August 2012

Annex A

THE TYPES OF PATIENT DATA USED IN HEALTH RESEARCH

Health data can be accessed by researchers in the following forms:

- *Identifiable data*—these include information in patient records such as patients' names, addresses, dates of birth and NHS numbers. There are also aspects of health data that could become identifying when they relate to a diagnosis of a rare condition or when combined with other data. Identifiable data are needed when future contact is needed with the participant, for example to contact them to take part in a study, or to link information across different data sets.
- *Key-coded or pseudonymised data*—these cannot directly identify an individual, but are provided with an identifier that enables the patient's identity to be re-connected to the data by reference to a separate database containing the identifiers and identifiable data. Pseudonymised data can often be used in place of identifiable data.
- *Anonymised data*—these data cannot be connected to the original patient record. Anonymised data are suitable when no contact is needed with the participant or where the data does not need to be linked to any other data sources.

Written evidence from CIFAS

INQUIRY INTO EUROPEAN UNION DATA PROTECTION FRAMEWORK PROPOSALS

1. Thank you for the opportunity to respond to your inquiry into the EU's Data Protection Framework Proposals.

2. As you will be aware, CIFAS is a not-for-profit membership association representing both the private and public sectors. We are dedicated to the prevention of fraud, including staff fraud, and the identification of financial and related crime. For over 20 years CIFAS has brought together a range of private sector organisations to limit fraud losses and protect consumers. We have over 260 Members with five public sector organisations having joined since 2010, namely the BIG Lottery Fund, Financial Services Authority, Legal

Services Commission, Student Loans Company and the UK Border Agency. The National Audit Office is an Affiliate Member.

3. Our response to your inquiry focuses on the impact the proposals on organisations which hold and share fraud data in order to prevent fraud and fraudsters.

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

4. CIFAS is broadly supportive of the EU's efforts through this regulation to create an effective system of data protection in the EU. The proposed regulation puts forward a number of steps to strengthen online privacy rights and protect individuals. Some of these proposals give us pause, however, lest they lead to a more restrictive regime which, under the guise of protecting individuals, actually provides a shield for fraudsters.

Consent

5. While CIFAS has no concerns over the revised definition of personal data as it stands, CIFAS is concerned that there should be proper clarification surrounding the proposed changes to the rules of consent to make quite clear that data controllers such as government departments and fraud prevention agencies, for example, are not left without a lawful basis for processing data which is necessary for the identification of crime and prevention of fraud.

6. If explicit consent to use data for fraud prevention purposes were to be required then a number of scenarios could emerge:

(a) A concerned few refuse. Those who do would be likely to have severe difficulty doing business with anyone because their risk would be seen as being unacceptably high. Any online service where fraud and identity checks were required would throw up these issues. Government should be wary about excluding sections of society from every-day transactions due to their concerns over personal privacy.

(b) Organised and other fraudsters refuse to give consent, making it impossible for fraud prevention agencies to match data to indentify them.

(c) A significant part of the population refuse consent, making it difficult for both the public and private sectors to deliver services online or using remote delivery channels.

7. In addition, explicit consent has a potential resource implication. For example, an organisation will currently process data on behalf of its staff under implied permission for a number of reasons set out within current legislation (but without explicit permission) such as the sharing of data with HMRC. Establishing such permission may require the redrafting and issuing of contracts and other documentation, the taking of legal advice and all of this would have significant resource implications.

8. Finally, CIFAS' experience with its Members suggests that policies such as Fair Processing Notices (FPNs, otherwise known as Privacy Notices) are being condensed as much as is possible as consumers do not wish to read or hear too much information before applying for a product. Indeed, in sectors where competition is high and consumer expectations equally so, the attitude is often "the shorter the phone call or text, the better". The EU needs to take the opinion of the silent majority of consumers into consideration when revising these proposals.

Data Breaches

9. CIFAS agrees that the notification time around data breaches needs to be defined. Reporting withinHow 24 hours seems to be an unreasonable requirement, however. Often it can take longer than this to ascertain the extent of the breach. CIFAS notes that the EU is stating that this approach should be taken "where feasible" so we suspect that they recognise this issue already.

10. CIFAS would suggest that telling the ICO about the breach and then laying out the steps taken to protect the individuals at risk, locate the missing data, and introducing procedures to ensure that this does not happen again would be a more complete way to report a loss than simply informing the ICO after 24 hours.

11. CIFAS therefore supports the approach set out under the "next steps" section on page 35 of the call for evidence.

Subject Access Requests

12. CIFAS strongly opposes the proposals around the removal of the fee for Subject Access Requests (SARs). We believe that the removal of the £10 fee would lead to a significant increase in SARs. Currently the £10 fee discourages vexatious requests while almost covering our costs.

13. CIFAS processed 1,210 SARs in the past 12 months. Based on an average processing time of 20 minutes, each request costs us £12.50. Costs to other UK businesses will vary but we believe that many will come out above £10. The cumulative effect of this proposal, if enacted, would therefore have a significant effect on UK

Plc. CIFAS is therefore pleased to see that the UK Government will resist the proposal for removing the fee for SARs.

14. In addition, however, CIFAS is concerned about the EU's proposal that "where the data subject makes the request in electronic form, the information shall be provided in electronic form". In actuality, this directive may cause additional administration for some compliant organisations (particularly SMEs) as they may not be able to perform the entirety of the transaction by email. Organisations that process SARs have an obligation to ensure that they release data only to the named individual. To comply, companies use a variety of identity verification methods. Large organisations can, for example, use electronic verification provided by a credit reference agency. Smaller organisations generally do not use such services. Instead, they have to find a less slick solution. Many, for example, request two pieces of identification documentation. These will be delivered and, in some cases where original documents such as driving licences have been supplied (which often happens, even where a photocopy has been requested), returned by secure post or, in the case of an original utility bill, by ordinary post. As an email address does not offer any reassurance of identity, it will be necessary to perform these same processes for online requests. In such situations, for consumers this will seem like an unnecessary and costly delay, and for processing businesses it will lead to additional costs as online applications and postal documentation will require linking. CIFAS therefore suggests that this aspect of the proposals requires further attention, to acknowledge that SMEs cannot avail themselves of some of the more sophisticated online identity verification products.

15. CIFAS believes that the price of SARs should be linked to an average processing cost from across the EU and linked to inflation, rounded to the closest 50p in sterling or 50c in euros to ensure that the figure remains sensible. As things stand at present, the value of the fee is effectively being eroded over time. CIFAS would also consider refunding SARs where the request discovered an error in favour of the requestor, but in our experience such situations hardly ever occur.

Right to be forgotten

16. CIFAS finds no reason to object to this proposal. It is our firm view, however, that it is important to create a very specific definition of "legitimate grounds" in order to ensure that requests to be forgotten are legitimate and do not cause a disproportionate rise in administration and legal costs. Data held only to record or prevent crime and frauds should be exempt, for obvious reasons. The Government's proposed "next steps" on this therefore seem eminently sensible.

Issuing of fines for organisations in breach of the regulation

17. CIFAS would suggest that fines should be linked to the actual damage caused and level of complicity of organisations in breach of the Act. We agree that punishments should be fair and proportionate, and that a catch-all such as that proposed by the EU is therefore fundamentally wrong. There should be scope to ensure that a company or organisation deliberately or maliciously in breach of the Act should be treated differently from an accidental breach where an organisation had taken reasonable steps to minimise risk, and in such cases there should also be scope to consider the impact of the punishment on the organisation.

18. The figure and percentage of annual turnover proposed in the draft regulation are arbitrary and could lead to an unfair burden on small businesses. For a small organisation, up to €1m may in fact be 20% of turnover, whereas 2% of turnover is €100,000, so the structure of fines must be set out very clearly so as not to discriminate against small organisations.

Will the proposed Directive strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection for police and criminal co-operation in the EU, and on the other for law enforcement authorities to be able to investigate crime without disproportionate financial or administrative burden?

19. Please see our comments under paragraphs 5 and 6 above, as these are equally relevant here.

Appointment of Data Protection Officers

20. CIFAS considers that ensuring that organisations define "who is responsible for what" in relation to data protection is a positive move. We do not support the need for a full-time DP Officer, however, and would suggest that data protection may be better managed if, once practical criteria are defined with which companies or organisations must comply, they are then left to decide whether an individual or a team has responsibility for maintaining the required standard. This could be done in an auditable way.

21. For an organisation such as CIFAS, working in the fraud arena, all staff require good data protection knowledge, and we would want to ensure that this standard was maintained rather than delegate responsibility limited to a single individual. CIFAS was therefore pleased to note that the Government will resist this aspect of the proposals.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

22. CIFAS considers that the next steps proposed by the Government appear, at this stage, to be sensible and proportionate. Certainly, the correct balance has been struck in ensuring that unnecessary burdens are not placed on business while protecting the rights of individuals.

23. CIFAS would support the Government's negotiating position on Subject Access Requests, the right to be forgotten, resistance to unwarranted burdens on industry, data breach notifications, strong supervisory authorities, penalties for breaches, and removal of powers from the EU.

24. We would, however, prefer that the Government took a robust stance on any new requirements on explicit consent and transparency: it will be essential to ensure that protections are in place (as they have been under the current regime) to ensure that these are not framed in such as way as to result in the shielding of criminals and fraudsters.

August 2012

Written evidence from the NHS European Office

EUROPEAN UNION DATA PROTECTION FRAMEWORK PROPOSALS

THE NHS EUROPEAN OFFICE - WHO WE ARE AND WHO WE REPRESENT

This response has been prepared by the NHS European Office. The NHS European Office is based in Brussels and London and is part of the NHS Confederation. The Office monitors EU policy and legislation which has the potential to impact on the way the NHS operates. It analyses key EU proposals and lobbies the European Institutions to influence them in the interests of the NHS.

EXECUTIVE SUMMARY

The NHS European Office welcomes the European Commission's revision of the existing EU Data protection laws, particularly in light of technological developments since the last Directive was implemented. However the proposed Regulation lacks clarity in a number of major areas of importance including for example consent .and the precedence of Union or Member State law. Although the proposal is for a Regulation we strongly believe that in order to best meet the needs of all those involved in data processing, including data subjects themselves, deferral to national law must be a possibility in a number of areas.

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

1. While the proposals make a solid attempt to introduce an up to date and practicable system of data protection in the EU, the overall task of harmonizing the way data should be processed across the EU as a whole is so immense that the proposals inevitably fall short in certain areas.

2. It is hard to assess whether the proposals "strike the right balance" between data protection and administrative burden, as perspectives on what the balance should be will vary greatly between the different types of organisations affected. Gaining explicit consent from a parent or guardian on behalf of a young person under the age of 18 for example, should be considered differently in the context of delivering health or social care, from the context of a social networking website.

3. Even within .an organisation as large and diverse as the NHS there will be differences of opinion on how certain types of data should be processed and who should have access to it. The context in which data is processed can be as important as the data content and allowances must be made for national law to decide what the best system of data processing would be in certain circumstances.

4. To their credit the European Commission has made a significant number of allowances in the text for Union law or Member State law to decide the way data should be processed, however there are major discrepancies within the text where responsibility has been devolved to national level (for example Rights of Access) and where extreme levels of detail are set at EU level (for example with regards the employment conditions of Data Protection Officers).

5. This inconsistency leads to confusion in the framework or a Regulation, and while it may be too late to make the transition, we question whether a revised Data Protection Directive may not have been a more effective and workable approach. This would have allowed national governments to ensure that public authorities' data processing systems had the opportunity to upgrade and improve whilst not being challenged by the EU's wider objective to cope with the overwhelming mass of data generated by the introduction of social networking sites and internet search engines. The proposals certainly make more sense when read in the context of Google or Facebook, as opposed to the way a clinician documents the course of a patient's treatment.

6. With this in mind, we welcome the Commission's attempts to deal specifically with personal data relating to health, and in relation to research. However, additional work is needed to add clarity to the text in both of these areas, particularly in relation to consent, data portability, the right to be forgotten and documentation.

7. Where consent is concerned it is not always clear when the European Commission expects consent to be explicit and where it may be implied, particularly in the context of healthcare and research.

8. Data portability requirements threaten to offer a lesser degree of protection to data subjects in the long run and to leave healthcare providers liable for data breaches unless provisions are introduced to guarantee the authenticity of the data transported and the security of the transportation process.

9. It is not clear to what extent the right to be forgotten may apply to health records. In this context it may be unhelpful and, at worst, damaging to the data subject (if for example, data is erased which may be critical to the health of the subject). It is impractical to implement.

10. Criteria relating to documentation are over ambitious and unrealistic in a healthcare setting. It is not always possible to determine in advance all those who may be involved in processing data or to define precisely who may be responsible for what.

11. We recognize that it is not the Commission's intention to increase the administrative and regulatory burden on the NHS in the field of data processing but there is still a significant amount of work to be done to ensure that the forthcoming regulation is clear, proportionate (particularly in terms of costs and fines), and appropriate for the NHS.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

1. The NHS European Office fully supports the next steps proposed by the UK Government. We recognize the need to update the existing legislation in light of the way technology has evolved and the way data is processed. We support improvements in the transparency of data processing and the Government's position in relation to access requests. Furthermore we agree with the position put forward by the Ministry of Justice concerning the right to be forgotten, an aspect of the text which we consider unrealistic and potentially unhelpful for healthcare providers and data subjects. As stated above we are concerned by the introduction of new bureaucratic and costly burdens on organisations which do not appear to offer greater protection for individuals. Furthermore there is a need to ensure that provisions made mandatory by the new Regulation do not incur a lesser degree of protection than conditions that are already in place.

2. Finally, the NHS European Office is strongly in support of UK Government proposals to remove many of the powers assigned to the European Commission to make delegated and implementing acts. This is important as it will help to limit additional changes to the Regulation in future which could have a significant impact on the way data is processed in the UK. We welcome this opportunity to raise our concerns with the Select Committee.

August 2012

Written evidence from the Advertising Association

EU DATA PROTECTION FRAMEWORK PROPOSALS

Introduction

The Advertising Association

1. The Advertising Association (AA) is the only organisation that represents all sides of the advertising and promotion industry in the UK—advertisers, agencies and the media. In the UK, the advertising industry directly employs over 300,000 people. In 2011, advertising expenditure was £16.1 billion.

2. We promote and protect advertising. We communicate its commercial and consumer benefits and we seek the optimal regulatory environment for our industry. Our goal is that advertising should enjoy responsibility from its practitioners, moderation from its regulators, and trust from its consumers.

Overview

3. This submission relates only to the Regulation for general and commercial data protection. We believe that this draft Regulation presents a serious threat to the advertising sector and, while accepting that the parallel Directive is an important legislative area, would like to ensure that enormous impact that the draft Regulation could have on our sector is recognised by the Committee.

Response to Terms of Reference Questions

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

4. We welcome the Inquiry's Terms of Reference which recognise the need to strike a fair balance between the rights of the individual to ensure that their personal data is protected and the rights of businesses to engage with consumers. In the current draft Regulation that balance is unfair and ultimately places unreasonable (and to some extent impossible) requirements upon businesses.

5. We support laws that work to protect consumers' personal data and we believe that updating the current law on data protection in light of the progress in digital technology is sensible. We, however, do not think the proposed EU-wide Regulation in its current form is an effective way to address this need.

6. The draft Regulation appears to lead to a regulatory regime that would make business operations more expensive and difficult. This could potentially undermine entire advertising businesses and the businesses that advertising supports and drives, and, ultimately, significantly impinge on growth and innovation in the economy. The Advertising Association is working with the industry to develop figures showing the potential impact of the Regulation, and one figure so far produced by the Direct Marketing Association suggests that it could cost the UK economy up to £47 billion.[26] Given this is a study by just one part of the broad advertising eco-system, the cost for our industry could be extremely high.

7. We are seriously concerned about the content of the draft Regulation which we believe could significantly burden businesses and hinder growth in the advertising industry, in particular the direct marketing and digital sectors. We reject the European Commission's premise that it will lead to a net saving for companies estimated at €2.3 billion and call on the Commission to provide a clearer evidence base that shows where these savings may come from and also recognises the costs to businesses from the new measures that they are proposing. Our assessment is that the Regulation could stifle innovation and increase costs and thus nullify any potential economic benefits to businesses. We recognise that businesses benefit from more consistent rules across Europe but question how realistic the draft Regulation's ambition to lead to laws being genuinely consistent across all member states actually is.

8. The Advertising Association believes that the European data protection legislative framework should remain high level, with the Commission focussing on inconsistencies of application and enforcement across the EU. The Commission's attempts to legislate for the current digital age are likely to become quickly out of date and we encourage the Commission to focus on a principles-based legal regime that can evolve as technologies develop.

9. The Commission must recognise that consumers benefit from a principles-based legal regime which ensures people's data is protected, while still giving them the benefits from the services and goods supplied to them through the data-driven economy.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

10. We are pleased that the UK Government recognises the threat that this Regulation poses to industry, and welcome the recognition of the advertising industry's concerns about the Regulation in the Government's response to the Call for Evidence submissions.

11. Naturally, we do not know the detail of the UK Government's focus in Council negotiations but our understanding is that they are taking a proportionate approach which is one we support. This approach is also shown their next steps as set out in the Summary of responses document and in general these are next steps that we support.

12. In particular, those areas raised by Government which we support relate to: concerns about increased bureaucracy and business costs, concerns about the workability of the right of be forgotten, and concerns about the excessive number of implementing acts:

12.1. *The bureaucratic and financial burden on businesses (especially SMEs who make up a large part of our sector) due to extra staff and possible sanction*: The advertising industry would be severely impacted by the bureaucracy and sanctions that are required in the draft Regulation. These burdens include: hiring a Data Protection Officer, addressing the fact that they could be liable to a fine of 2% of their annual turnover, and processing the increased amount of data now classified as "personal". The Commission speaks of €2.3 billion savings for business. We dispute the idea that money will be saved but rather believe it will impose a lot of costs on businesses.

Additionally, UK companies benefit from a strong and effective Data Protection Authority in the ICO, and we are also concerned that the increased bureaucracy that the draft Regulation imposes on the Commissioner's Office will undermine their ability to act as an effective enforcement body. We would like to see a Regulation that enables the ICO to continue to be effective through being independent and being able to make decisions based on genuine risk.

[26] http://www.dma.org.uk/toolkit/putting-price-direct-marketing&usg=AFQjCNG6WzQfZDL-4A0C7qLIlgjPMA8I-A

12.2. *The introduction of a "right to be forgotten"*—The advertising industry, and particularly the direct marketing sector, is concerned about the proposed right to be forgotten, and specifically its impact on third party data list brokers. The current data protection laws already set out rules that provide people with information on the identity of the organization processing their personal data, and the purposes of this. Articles 12 and 14 of the current Directive provide a right of access and a right of objection. Individuals can require their personal data to be erased, blocked, changed or deleted. The proposed Regulation would require companies that hold an individual's data and pass them to third parties to not only have to delete their information, but also to ensure the third party deletes this information too.

The introduction of the phrase of a "right to be forgotten" sets unrealistic expectations to the consumer as to what is achievable as it is often simply impossible for data on the internet to genuinely be "forgotten" as this data may be shared by a number of actors out of the control of the original data processor. There is certainly a need to provide greater information to people about their rights to erase data and to advise people but creating unrealistic consumer expectations is not a worthwhile exercise.

12.3. *The extension of powers to the Commission through "delegated" and "implementing acts"*—The Commission has included many of these acts which enable it to eventually amend the Regulation without any proper industry consultation or checks and balances of an orderly legislative process. This leads to increased business uncertainty about the future shape of data protection law in Europe. Furthermore, the lack of proper consultation with industry is extremely worrying and will continue to deepen the problematic issues around the democratic accountability of the Commission.

13. In addition to those areas raised by the Government in their document, we have particular concerns about the impact on our sector by new extending the definition of personal data and by mandating unworkable consent requirements:

13.1. *The definition of personal data (eg including some IP addresses & cookies as personal data) and consequences for profiling*—The draft Regulation proposes a blunt catch-all definition of personal data. In doing so, it proposes that some cookie data and IP address data should be considered "personal". We believe this is an unreasonable approach as in many cases, IP addresses and cookies are not directly linked to an individual. This new Regulation makes no distinction between this type of data (which is not directly identifiable) and directly identifiable information (eg full postal address). The use of cookies and IP addresses is essential to the smooth running of the internet. It is also necessary for the delivery of targeted advertising that is relevant to a browser but that uses no directly identifiable data. The personalisation of these data sets could be very damaging particularly if the consent requirements are interpreted to require explicit consent for the processing of cookie data. Furthermore, the impact on the consumer of having what is currently "anonymous" data, like cookie data, considered "personal" could undermine the way in which clearly identifiable personal data is processed as businesses are forced to treat these data sets equally and are therefore overwhelmed with vast quantities of data.

We call for the UK Government to advocate a risk-based approach that addresses the issue of personal data based on the likelihood of identification of an individual rather than a blunt catch-all definition. This more granular approach has been advocated in ICO's code of practice on Personal Information Online. Developing this concept further, we believe that both business and consumers would benefit from an approach that considers recognising a category of data which is not directly identifiable but neither is completely anonymous. Rules should be created for the processing of such data but they should be proportionate and therefore not be as onerous as the rules that are required for processing of directly identifiable personal data.

13.2. *The requirement for explicit and informed consent for data collection & processing*-As raised above, any moves to require "explicit" consent for processing of cookie or IP data should be avoided. This would lead to increased "opt-in" mechanisms for the collection of what are effectively anonymous data sets. Businesses would essentially be forced to personalise these data sets in order to obtain the explicit consent of users. This is both hugely burdensome for companies and would severely undermine the consumer's online and offline experiences. From a practical point of view, it would lead to multiple pop-ups online for cookies and hugely affect the direct marketing industry with the likely impact being an increase in unaddressed mail.

Taking the cookies issue specifically, industry is working hard to comply with the consent requirements set out in the ePrivacy Directive, and so amending the consent requirements in this Regulation would further increase burdens. Therefore, it is critical that (as per Article 6 1. f in the draft Regulation), the processing of personal data can be lawful "if this is necessary for the purposes of the legitimate interests pursued by a controller". We accept that such interests can be overridden by the rights and freedoms of the data subject, in particular where the data subject is a child. Any moves to require explicit consent for the processing of categories of data that are unique to a device—like cookies—but that do not directly identify an individual would be severely detrimental to the UK economy.

August 2012

Written evidence from the Association of British Insurers

EUROPEAN DATA PROTECTION FRAMEWORK PROPOSALS

1. The ABI is the voice of UK insurance, representing the general insurance, protection, investment and long-term savings industry. It was formed in 1985 to represent the whole of the industry and today has over 300 members, accounting for some 90% of premiums in the UK.

Executive Summary

2. The proposed EU data protection:

- Will reduce some existing administrative procedures undertaken by firms, such as, for example, simplification of notification filings. However, these changes do not outweigh the additional burdens being placed on businesses with no discernible benefit to individuals. We believe that the measures proposed should be proportionate to the nature and size of the business and level of risk to privacy involved.
- Must explicitly recognise the need for organisations, including insurers, to share information to prevent fraud and other financial crime. In 2010, UK general insurers detected 133,000 cases of fraud with a value of £919 million. But around £2 billion in insurance fraud goes undetected each year, adding, on average, an extra £50 a year to the insurance bill paid by each UK policyholder.
- Creates confusion about the scope of the right to be forgotten for consumers and individuals. The right to be forgotten must be appropriately designed to ensure that: consumers are not misled, it cannot be exploited for fraudulent purposes, it respects contractual obligations, and reflects data retention requirements, as required by law.
- Should be amended to reflect a pragmatic and proportionate approach to requirements such as data breach notification, application of sanctions/fines, mandatory data protection impact assessments, and responding to subject access requests. In its current form, the proposed EU data protection regulation would not be meeting its aims of delivering an effective and proportionate approach for both citizens and businesss in the EU.

3. We welcome the approach proposed by the UK Government, particularly on issues such as subject access requests and the right to be forgotten. However, in addition, the Government should seek to ensure that vital consumer protection measures such as fraud prevention and detection are not inhibited and thatinconsistencies and duplications are resolved.

Introduction

4. The ABI welcomes the opportunity to input to the Justice Select Committee inquiry on the EU data protection proposals.

5. The proposals are a key consideration for the insurance industry. Insurers recognise the importance of data privacy and take their responsibility for data protection seriously. We welcome the aim of the Regulation to create a uniform regime for data protection across the EU, and the intention to reflect technological advances. However, as currently drafted the Regulation will have a disproportionate impact on businesses which provide important services to consumers without delivering the benefits intended for individual data subjects.

6. Insurers need the ability to access, process and store data in order to provide consumers with the right products at the right price. Using the data enables insurers to determine the level of cover needed and to then set an appropriate premium tailored to that customer. The insurance industry, and the consumers it serves, will be negatively impacted if the new proposals restrict their ability to use the data effectively for these purposes.

7. The proposed Regulation does not differentiate between those, such as the financial services sector, which are already extensively regulated, and other sectors, which are less strictly controlled. Financial services activity within the UK and throughout the EU is subject to a substantial range of primary and secondary legislation, as well as rules and guidance issued by the financial regulators. We are concerned that the proposed Regulation may conflict, or be inconsistent, with existing rules and regulations to which financial institutions are subject. Data protection legislation must be flexible enough to work in harmony with existing EU and member state financial regulators rules and regulations.

8. The Commission estimates that European businesses will benefit to the tune of €2.3 billion from the proposed changes. We do not believe that harmonisation in the way proposed will deliver that magnitude of savings. The Regulation increases the number of requirements placed on business. The added costs of compliance will wipe out any potential savings and are likely result in much higher overall burdens.

Question: Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

9. We do not believe that the proposed Regulation will deliver a proportionate, practicable or effective system for data protection in the EU. The following key points are vital for the insurance market in being able to continue to provide adequate, appropriate and affordable products to its customers.

Data Sharing for Fraud Purposes (Article 6/9)

10. Detecting fraud protects honest consumers. It is therefore important that efforts to combat fraud are supported and explicitly recognised in the development and application of the Regulation and not restricted as currenty proposed.

11. Reducing and deterring insurance fraud is a priority for the insurance industry. In 2010, UK general insurers detected 133,000 cases of fraud with a value of £919 million. We estimate that around £2 billion in insurance fraud goes undetected each year, adding, on average, an extra £50 a year to the insurance bill paid by each UK policyholder.

12. We are extremely concerned that changes to the EU data protection legislative framework may impact on the ability of insurers to share information for these purposes. Given the importance of fraud prevention and its benefit to consumers, it should not be left ambiguous or vulnerable to interpretation. It is therefore important that efforts to combat fraud are supported and explicitly recognised in the Regulation.. Whilst we believe that Article 6, Clause 1(f) for non-sensitive data,[27] encompasses data sharing for fraud purposes, 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, which can be an important component for insurance fraud detection or prevention.

13. There must be reassurance through clarification in Article 9 that the definition of a "task carried out in the public interest" (Article 9, Clause 2(f)) includes data processing for anti-fraud purposes. If this is not the case, the Regulation should explicitly recognise the need to process data for these purposes through the inclusion of a specific exemption where processing is necessary for the purposes of preventing fraud.

14. The use of criminal convictions data is also vital for insurance fraud detection. Furthermore, we seek reassurance that rules on profiling (Art 20) in combination with Article 9 requirements will not prohibit insurers from processing data concerning offences or criminal convictions (with the individuals consent). This is an important component of the underwriting process. Premiums are calculated on the basis of risk and evidence shows that relevant unspent convictions can indicate the likelihood of making a future or a fraudulent claim. Restricting insurers' ability to use this information will impact on lower risk consumers as it would inhibit the insurers ability to weight according to risk. This would potentially result in premiums rising for all policyholders. This would not be fair to the consumer and it would be a disincentive on individuals to act responsibly.

Proportionality

15. We recognise that some proposals will reduce some of the existing administrative procedures undertaken by firms, such as simplification of notification filings, and reduced requirement for transfer permits. However, these changes do not outweigh the additional burdens being placed on businesses with no discernible benefit to individuals.

16. We believe that the measures proposed should be proportionate to the nature and size of the business and level of risk to privacy involved. The following are examples of areas which we view as disproportionately onerous and significantly increasing the burden of for data controllers:

- mandatory data privacy impact assessments (Article 33).
- breach notification (see paragraphs 23–26) and administrative sanctions (Art 79).

17. The obligation to undertake a data privacy impact assessment (DPIA) is unnecessarily bureaucratic and broad. The requirements are overly prescriptive, particularly the stipulation that data controllers "seek the views of data subjects or their representatives on the intended processing". This will have the effect of turning an internal good practice activity into a formal, externally monitored requirement. In addition, the circumstances where a DPIA is required have not been clearly defined. We believe that the onus should be on the Data Protection Authorities (DPA) to assess if a legal obligation placed upon the data controller presents a specific risk to the "rights and freedoms of the data subject".

18. In relation to the administrative sanctions, the broad areas where fines can be applied are disproportionate in relation of the risk of harm to an individual that might arise from a breach of the Regulation. DPAs do not have discretion when deciding to impose a fine. For instance, the DPAs are obliged to impose a fine ("shall impose a fine") even if the violation has not produced any damage to the data subject or to consider any other mitigating circumstances. This would lead to situations where a fine of up to 0.5% of annual worldwide

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

turnover (which would run into millions for some financial services providers) will apply for responding a few days late to a request for access to personal data.

19. We agree with the Information Commissioner's Office (ICO) that there should be a demonstrable link between the breach in question and the impact on data privacy. The levels of fines should be revised. The test for whether a fine is warranted, and if so the level of fine, should be the presence of a demonstrable link to the impact on privacy associated with the breach.

Profiling (Article 20)

20. Any rules on "profiling" should not prohibit or restrict the ability of insurers to conduct a risk assessment on the basis of the information provided to determine the appropriate level of insurance cover and price for the individual. Risk assessment is a key element of how insurers use data to determine whether cover can be provided, the level of cover needed and to then set an appropriate premium tailored to that customer.

21. We are particularly concerned that Article 20(3) will prohibit insurers from processing (with the individuals consent) data concerning offences or criminal convictions. This is an important component of the underwriting process, evidence shows that relevant unspent convictions can indicate the likelihood of making a future or a fraudulent claim.

22. Restricting insurers ability to use this information will impact on lower risk consumers as it would inhibit the insurers ability to weight according to risk. This would potentially result in premiums rising for all policy holders. This would be detrimental to the consumer and is no incentive on individuals to act responsibly.

Breach Notification (Article 31)

23. Insurers take their responsibility with regard to data breaches seriously. They have internal processes in place to identify, record, investigate and respond to any data breaches that may occur. Under the Commission's proposals, there would be a mandatory requirement to notify the Data Protection Authority (DPA) of any data breach within 24 hours or provide justification of why a breach cannot be notified with this time limit. This would mean that circumstances where the breach poses little or no risk to the individual—eg a letter containing marketing information is sent to the wrong address—are included. This is disproportionate, and would result in a heavy administrative burden for businesses and the DPA, and would not deliver benefits for the consumer.

24. We support the UK Government's position on this issue, which advocates a degree of proportionality. We consider that only breaches that pose a significant risk of harm to data subjects—and where data subjects should take action (eg to prevent identity theft) or remain vigilant—should be notified. It should be noted that regulated financial services companies in the UK already have an obligation to notify those data security incidents to the FSA which may create a heightened risk of financial crime, or which affect the company's ability to provide adequate services to its customers and result in serious detriment to any customer, or have a significant adverse impact on the company's reputation. In practice, the company would also notify the ICO.

25. We agree with the ICO that notification requirements should be "without undue delay" rather than within a stipulated timeframe. This is in line with the e-Privacy Directive approach and the approach set out for consumers in the new Regulations.

26. The Regulation should reflect a pragmatic and proportionate approach to notification such that only serious or significant breaches are notified to the DPA without undue delay rather than specify a time limit.

Right To Access Data (Article 12)

27. We agree that an individual's right of access should be user friendly. However, we oppose the removal of the right to charge a fee. We are pleased to see the UK Goverment is supportive of this position. This £10 fee does not meet the administrative costs of handling a request; however, it is widely recognised that it does go some way towards deterring frivolous or malicious SARs (which are submitted in order to cost the business time and money). It may also deter, for example, claims management companies and fraudsters from seeking to obtain high volumes of consumers data. In practice, in our members' experience, the SAR mechanism is only rarely used for the purposes for which it was intended (protection of privacy). It is much more widely used to conduct fishing expeditions with a view to litigation.

28. We are also concerned about the lack of flexibility in the timescales for responding to complaints. The right of access requires a data controller to take account of many obligations and considerations when responding to a request. This includes locating the source of data, the form in which the information should be provided, redaction of third party data, or the application of legal exemptions. In addition, access requests received by insurers can be complex, be it in terms of the volume or nature of information requested eg a request from a customer who has held a life insurance policy with the firm for 20 years for "all data" relating to them. The proposed Regulation stipulates that all access requests must be responded to within one month (this is a reduction on the current limits). We believe there should be flexibility within the Regulation where requests are manifestly excessive, for example due to their complexity or the amount of data to be retrieved.

RIGHT TO BE FORGOTTEN (ARTICLE 17)

29. We agree with the UK Government's intention to push for an overhaul of the "right to be forgotten". There is confusion about its scope for both organisations and individuals. The "right" is misleading for consumers as many forms of customer data held by insurers and other financial services providers are required to be held for specific periods by law. Requests from consumers to have data removed would have to be denied where such data needs to be kept by the insurer under the provisions of other legislation, leading to complaints and litigation.

30. Clause 4(b) of Article 17 states that where it is necessary for a data controller to retain the data, instead of erasure, the controller "shall restrict processing where the controller no longer needs the data for the accomplishment of its task but they have to be maintained for purposes of proof". It is not clear what the "restriction" of processing means, and the extent to which an organisation would be able to retain and use data. For example, in defending legal proceedings, responding to a complaint raised by a customer or through an alternative dispute resolution scheme.

31. Accordingly, 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; and
- it recognises the need for organisations to retain data for specific periods, as required by law.

DATA PORTABILITY (ARTICLE 18)

32. The inclusion of requirements on data portability is a substantive and concerning addition, and it is highly questionable whether it should fall inside the scope of this Regulation as it is not about data protection or security.

33. Its inclusion has implications for competition and intellectual property, raises issues relating to standardisation and has potential cost implications for businesses. For example, this could unintentionally require insurers to disclose commercially sensitive information, such the critiera used to price policies according to the individual's needs.

34. The ability to change providers easily is a consumer and/or competition issue and should be dealt with under other relevant legislation at which point any data protection considerations can be taken into account.

Question: Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

35. It is imperative that the UK Government press for a more proportionate approach to regulation that does not over burden businesses where there is no benefit to the individual data subject.

36. We welcome the approach proposed by the UK Government. However, in addition to the areas identified we urge the Government to ensure the regulation:

- Will not inhibit the ability of financial services providers from sharing data to detect or prevent fraud and financial crime.
- Provides sufficient flexibility to allow organisations to respond to SARs rather where they are complex, manifestly excessive or involve large amounts of data.

August 2012

Written evidence from International Regulatory Strategy Group's

EUROPEAN DATA PROTECTION FRAMEWORK PROPOSALS

SUMMARY

- The IRSG recognise that there is a need to update the existing Data Protection Directive (95/46/EC), however we do not think that the new proposals will deliver an effective system for data protection across the EU.
- Our response focuses on four key themes: the accountability of data controllers, proportionality, how financial services providers need to use data, and the international/extra- territoriality effect of the proposals.
- Our main concerns are that the proposed Regulation:
  - will place significant additional burdens on organisations without delivering discernible benefits for data subjects;
  - may be inconsistent with and/or duplicate existing laws and regulation in the UK and internationally;
  - may affect consumer protection measures to prevent or detect fraud or financial crime; and

— may impact on the inward business investment into the EU.

— We welcome the approach proposed by the UK Government, particularly on issues such as subject access requests and the right to be forgotten. However, in addition to the areas identified, the Government should push the European Commission to resolve inconsistencies and duplications and ensure that vital consumer protection measures such as fraud prevention and detection are not inhibited.

Introduction

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

2. We recognise the need to update the existing legislation and welcome the opportunity to input to the Justice Select Committee inquiry.

3. We welcome the aim of the Regulation to create a uniform regime for data protection across the European Union, and the intention to reflect technological advances. However, as currently drafted the Regulation will have a disproportionate impact on businesses which provide important services to consumers without delivering the benefits intended for individual data subjects.

4. The draft General Data Protection Regulation (GDPR) is targeted across all sectors and does not differentiate between those, such as the financial services sector, which are already extensively regulated, and those we believe to be the primary target for this measure, such as the sphere of social networking, which are less strictly controlled. Financial services activity within the UK and throughout the EU is subject to a substantial range of primary and secondary legislation, as well as rules and guidance issued by the financial regulator. We are concerned that the GDPR may conflict, or be inconsistent, with existing rules and regulations to which financial institutions are subject. Data protection legislation must be flexible enough to work in harmony with existing EU and member state financial regulators rules and regulations.

5. In addition, it is important that the Regulation recognises that varying degrees of risk and sensitivity may attach to data being processed. This should be reflected in the standard of protection expected to be applied to different categories of data. Not taking this into account could result in the imposition of an unduly administrative burden, relative to the associated risk.

6. There are a number of areas within the proposal which are not covered in detail in this paper but which nevertheless give cause for concern to the financial services sector eg the number of delegated/implementing acts which could introduce added bureaucracy and opacity, and delay implementation. We have omitted them because we recognise that these concerns are shared across other industry sectors. We intend to focus our comments on matters of specific relevance to the financial services industry.

Question*: Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?*

7. We do not believe that the proposed Regulation will deliver a proportionate, practicable or effective system for data protection in the EU. Our response focusses on four main areas of concern with the proposals.

Accountability

8. The new Regulation introduces rules aimed at bringing about greater accountability of data processors and controllers to ensure the principles and obligations of data protection are complied with. We believe that there is much to be gained from improving legal certainty through harmonisation of data protection rules within the EU. However, we are concerned that the current proposals are over-prescriptive and may ultimately place a greater compliance burden on business, with little or no additional benefit to individuals. Nor do we believe that this approach will necessarily lead to better data protection.

9. Whereas the existing Directive (95/46/EC) adopted a principles-based approach to data protection, the current proposals impose a set of rules in relation to the steps that data controllers should take in order to comply with these principles. For the most part these requirements do not take account of the nature and context of processing that is being carried out. For example, the proposed Regulation requires that justification of the purposes of processing, and the envisaged consequences of data processing, is presented to the customer on request. In many circumstances, it is very clear to the customer why certain processing is required, for instance in the case of a credit check if an application or a credit card is being made.

10. We believe that the specific and form-based nature of the measures proposed will in many instances lead to a superficial "box-ticking" approach to compliance rather than allowing those responsible for data protection to direct their resources towards effective data protection practices.

11. We agree with the Ministry of Justice's intention to push for an overhaul of the "right to be forgotten" (RTBF). There is confusion about its scope for both organisations and individuals. A RTBF is misleading for

consumers as many forms of customer data held by, for example, banks and insurers are required to be held for specific periods by law. Requests from consumers to have data removed would not be possible in these cases, leading to complaints and litigation. Equally, clause 4(b) of Article 17 states that where it is necessary for a data controller to retain the data, instead of erasure, the controller "shall restrict processing where the controller no longer needs the data for the accomplishment of its task but they have to be maintained for purposes of proof". It is not clear what the "restriction" of processing means, and the extent to which an organisation would be able to retain and use data. For example, in defending legal proceedings, responding to a complaint raised by a customer or through an alternative dispute resolution scheme.

12. Accordingly, 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; and
— it recognises the need for organisations to retain data for specific periods by law.

Proportionality

13. We recognise that some proposals will reduce some of the existing administrative procedures undertaken by firms. For example, simplification of notification filings, reduced requirement or transfer permits, Binding Corporate Rules to be formally recognised as an alternative transfer mechanism, the principle of single regulator for all EU processing (although not fully realised). However, these changes do not outweigh the additional burdens being placed on businesses with no discernible benefit to individuals.

14. We believe that the measures proposed should be proportionate to the nature/size of the business and level of risk to privacy involved. The following are examples of areas which we view as disproportionately onerous and will significantly increase the burden for data controllers:

— the requirements for information to be provided to data subject (Article 14);
— mandatory data privacy impact assessments (Article 33); and
— breach notification (Arts 31 & 32) and administrative sanctions (Article 79).

15. The obligation to undertake a data privacy impact assessment (DPIA) is unnecessarily inflexible and too broad in scope. The requirements are overly prescriptive, particularly the stipulation that data controllers "seek the views of data subjects or their representatives on the intended processing". This will have the effect of turning an internal good practice activity into a formal, externally monitored requirement. In addition, the circumstances where a DPIA is required have not been clearly defined. We believe that the onus should be on the Data Protection Authorities (DPA) to assess if a legal obligation placed upon the data controller presents a specific risk to the "rights and freedoms of the data subject".

16. The introduction of "explicit" consent under Art. 4(8) could constitute a major change, depending on what requirements it introduces in practice. Providing explicit consent for each separate purpose would be time-consuming for the consumer and resource-intensive and costly for businesses. Excessively long notices/consents will not be read by individuals and will therefore fail in their intended purpose, adding only a barrier and cost to services.

17. In relation to the administrative sanctions, the broad areas where fines can be applied are disproportionate in relation to the risk of harm to an individual that might arise from a breach of the Regulation. DPAs do not have discretion when deciding to impose a fine. For instance, the DPAs are obliged to impose a fine ("shall impose a fine") even if the violation has not produced any damage to the data subject or if it is the first violation or to consider any other mitigating circumstances. This would lead to situations where a fine of up to 0.5% of annual worldwide turnover (which would run into millions for some financial services providers) will apply for responding a few days late to a request for access to personal data.

18. In addition, within the financial services sector the processing of personal data will often relate to a very small proportion of the overall global business. We do not believe that a business should be disproportionately penalised because of an issue arising within a small proportion of its operations by imposing fines based on global turnover.

19. We recognise that there will be costs associated with the introduction of these new measures. We believe that the costs should not exceed the intended benefits. Whilst it is difficult to provide an accurate estimate of the likely costs of both initial implementation and subsequent monitoring of compliance, the additional provisions provide an additional layer of bureaucracy, which we believe goes beyond what is necessary, without leading to improved protection for individuals.

Uses of Data

20. The financial services industry must comply with a broad range of legislative and regulatory measures which require financial services providers to process personal data. As currently drafted, the proposed Regulation does not fully recognise the legitimate interest that businesses have in processing data to comply with extensive financial regulation which may not always have the force of law in the sense of Articles 6(1)(c)

and 6(3) in relation to anti money laundering, fraud, and IT security. We believe clarity is required that the proposed Regulation does not interfere with the ability of businesses to comply with regulatory and similar obligations. This may be best achieved by these uses of data being explicitly recognised in the drafting of the Regulation.

21. We are also extremely concerned that the proposals may impact on organisations' ability to process and/or share data to prevent and detect fraud and other financial crime. We support measures that ensure appropriate consumer protection, however it is fundamental that the Regulation recognises the validity of processing in these circumstances.

22. Detecting fraud protects honest consumers. For example, in 2010, UK general insurers detected 133,000 cases of fraud with a value of £919 million. The ABI estimate that undetected fraud adds on average an extra £50 a year to the insurance bill paid by each UK policyholder. Given the importance of fraud prevention, the processing of data for this purpose should not be left ambiguous or vulnerable to interpretation. It is therefore important that efforts to combat fraud are supported and explicitly recognised in the development and application of the Regulation, not restricted. Whilst we believe that Article 6, Clause 1(f) for non-sensitive data,[28] encompasses data sharing for fraud purposes, it is not clear whether there is sufficient flexibility in the Regulation for sensitive data to be shared for these purposes.

23. There must be reassurance in recitals or through clarification in Article 9 that the definition of a "task carried out in the public interest" (Article 9, Clause 2(f)) includes data processing for anti-fraud purposes. If this is not the case, the Regulation should explicitly recognise the need to process data for these purposes through the inclusion of a specific exemption where processing is necessary for the purposes of preventing fraud. Fraud prevention and detection is an important form of consumer protection.

24. 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 proposed Regulation needs to recognise this as a legitimate basis for processing and permit storing data on criminal convictions. It is not appropriate, as is currently implied in the proposed Regulation, to limit the legal obligations around storing data on criminal convictions. The use of criminal convictions data is also vital for insurance fraud detection. Furthermore we seek reassurance that rules on profiling (Art 20) in combination with Article 9 requirements will not prohibit insurers from processing data concerning offences or criminal convictions (with the individuals consent). This is an important component of the underwriting process. Premiums are calculated on the basis of risk and evidence shows that relevant unspent convictions can indicate the likelihood of making a future or a fraudulent claim. Restricting insurers' ability to use this information will impact on lower risk consumers as it would inhibit the insurers' ability to weight according to risk. This would potentially result in premiums rising for all policy holders. This would not be fair to the consumer and is no incentive on individuals to act responsibly.

International/Extra Territoriality

25. 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 (eg important provisions recently included in the EU-South Korea Free Trade Agreement). We believe that this is likely to act as a disincentive to non-EU firms from providing services into the EU, as the proposals make personal data processing less attractive to them. This will ultimately result in reduced choice for consumers. We therefore view the GDPR as a clear barrier to trade, and as such likely to have an impact on the EU's stance in international trade negotiations.

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

27. We fear that the current proposals could have an immediate impact on the inward business investment into the EU. This relates in particular to online services. The proposals mean that the regulation of personal data processing in the EU is made more onerous and such processing is therefore much less attractive to non-EU entities. As currently drafted they will apply to non-EU firms with solely non-EU based clients who wish to seek the services of an EU-based data processor. The proposed Regulation is a missed opportunity to recognise that EU data protection laws need not regulate processing just because it happens to take place on equipment in the EU or through the agency of a processor in the EU, when it has no substantive/purposive connection to the EU.

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

Question: *Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?*

28. The financial and professional services industry has significant concerns over the data protection proposals. It is imperative that the UK Government press for a more proportionate approach to regulation that does not over burden businesses where there is no benefit to the individual data subject.

29. We welcome the approach proposed by the UK Government as set out in the Summary of Responses. However, in addition to the areas identified we urge the Government to:

- Push for clarity that the Regulation will not interfere with organisations' ability to comply with existing regulation.
- Ensure the regulation will not inhibit the ability of financial services providers from sharing data to detect or prevent fraud and financial crime which provides important consumer protection.
- More explicitly recognise the need to take into account the evolving nature of technology, especially ensuring it is easier for data subjects to transfer data internationally for it to be stored and processed in different parts of the world.

August 2012

Annex I

INTERNATIONAL REGULATORY STRATEGY GROUP—DATA PROTECTION WORKSTREAM MEMBERSHIP

ABI.

AFME.

Aviva.

BBA.

Clifford Chance.

Citi.

DLA Piper.

Fidelity.

FLA.

HSBC.

IMA.

Lloyds.

Morgan Stanley.

PWC.

Promotory.

RBS.

RSA Group.

TheCityUK.

Thomson Reuters.

Written evidence from Thomson Reuters

EUROPEAN UNION DATA PROTECTION FRAMEWORK PROPOSALS

SUMMARY

1. The Regulation needs to recognise the different contexts in which personal data is processed. While certain measures may be appropriate in relation to data collected from a consumer acting in that capacity, they may not be appropriate for the use of personal data in other contexts.

2. *Financial crime*[29] including money laundering, terrorist financing and bribery and corruption is a global phenomenon and requires global coordination to ensure that the risks arising from it are mitigated. The risks

[29] money laundering, terrorist financing, aircraft hijacking, arms trafficking, bribery and corruption, counterfeiting, extortion, forgery, fraud, tax evasion, kidnapping, human trafficking, insider trading/market manipulation, narcotics related crime, organised crime, pharmaceutical related crimes, piracy, racketeering, securities fraud, smuggling, terrorism and war crimes

it poses do not stop at the borders of the EU. The EU has committed itself to continuing the fight against *financial crime* as demonstrated by a number of ongoing initiatives including the review of the anti-money laundering and terrorist financing directive (2005/60/EC).

3. Counterparty screening is an essential part of these efforts but the proposed General Data Protection Regulation ("Regulation") may impede such screening and so conflict with the EU's commitments.

4. It must be in the EU's interests to encourage and enable both EU and non EU entities to undertake public domain screening as part of their efforts to combat *financial crime*.

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

5. We do not believe that the proposed Regulation will deliver a proportionate, practicable or effective system for data protection in the EU because of its potential impact on the private sector's efforts to combat *financial crime.*

6. Commercial sector organisations (like World-Check) provide information solutions to their clients in both the public and private sectors. For example, all of the UK's high street banks use World-Check to undertake their anti-money laundering and counter-terrorist financing screening. While diverse in nature, what its clients have in common is a legal, regulatory or risk management responsibility to undertake customer or counterparty screening as part of their internal processes designed to combat *financial crime*.

7. Information solution providers aggregate and provide their clients with access to *public domain data* on individuals named on international sanctions list, Politically Exposed Persons (as defined by EU directive 2006/70/EC) and individuals named on law enforcement, regulatory or reputable media websites as being guilty or suspected of *financial crime*.

8. All information is found entirely online and could be accessed by any member of the general public.

9. The wide range of organisations that use this type of personal data include banks, insurers, other non-bank financial services organisations, lawyers, accountants and a wide range of corporates.

10. The Regulation does not recognise that this wide range of private sector organisations need to process data relating to criminal convictions and related security measures as its is at the heart of their screening processes designed to combat *financial crime*. While this type of data is quite rightly regarded as "sensitive" under the Regulation, organisations need to know if a potential customer is a money launderer.

11. Because this criminal convictions data is sourced from the public domain, it is impossible to obtain consent from the data subject and even if such consent could be sought, it would not be forthcoming. Therefore private organisations and those that provide information services to them must look for another lawful basis to process such data under Article 9 of the draft Regulation.

12. The Regulation does not clearly sanction the processing of criminal convictions data by:

(a) *non-EU organisations* that are now caught by the scope of the Regulation but need to process for compliance with their home state legal or regulatory obligations; or

(B) *EU organisations* processing because they are caught by the extra-territorial effect of non-EU legislation.

13. *The Regulation needs to be clarified so that such EU and non-EU organisations do not face uncertainty or a conflict between complying with those non-EU legal obligations and adhering to the restrictions in the Regulation.*

14. In addition, the Regulation does not clearly sanction the processing of criminal convictions if carried out by an EU or non-EU organisation for *non-statutory regulatory, good industry practice or risk management reasons*. Currently it requires that any processing of such data for public interest reasons must "have a legal basis in" EU or Member State Law (Recital 36).

15. Example; a UK company wishes to appoint a sales agent outside the EU. To ensure that the sales agent will not implicate it in bribery or corruption, the EU organisation chooses to undertake due diligence on the sales agent. The EU organisation is under no legal obligation to undertake such due diligence under the UK Bribery Act—it is recommended but not a legal obligation. The due diligence reveals evidence that the agent has a criminal conviction for bribery. It is not clear whether the processing of such information by the UK organisation is lawful under the Regulation.

16. *The Regulation should clearly recognise that organisations that choose (without being legally obliged) to carry out screening as a means of assisting them to prevent financial crime, have a lawful ground on which to do so.*

17. Therefore we would propose the lawful grounds for processing criminal convictions data should unambiguously *extend beyond legal or regulatory obligations based in EU or Member State law.* In our view,

the Regulation should recognise that it is in the EU public interest for organisations to process criminal convictions data for the purposes of preventing, detecting or investigating *financial crime*.

18. Under the existing Directive (Article 8(4)), Member States for reasons of *"substantial public interest"* are able to put in place additional exemptions in relation to the processing of sensitive personal data. The UK has done so under *Paragraph 1 of the UK Data Protection (Processing of Sensitive Personal Data) Order 2000/417* which legitimises the processing of criminal convictions data if the processing:

(a) is in the substantial public interest;

(b) is necessary for the purposes of the prevention or detection of any unlawful act; and

(c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.

19. *We would advocate that the ability of Member States to make such common sense derogations from the Regulation in the area of the prevention or detection of crime should continue.*

20. Even where processing is allowed for compliance with a legal obligation, the Regulation imposes additional burdens beyond the mere requirement to comply—such as requiring that if the legal obligation is imposed by a Member State, it must meet an objective of the public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued (Article 6(3)).

21. Are Member States expected and if so able to specifically amend their legislation in time to make sure it addresses these issues? That does not seem practical.

22. *It should be sufficient that a controller is obliged to comply or is seeking to avoid a breach of the laws of its Member State without further qualification.*

23. Finally, the Regulation should recognise that personal data that is in the public domain and so already widely publicly available in third countries has a different risk profile to data that is collected from data subjects. The provisions of the Regulation relating to International Data Transfers should recognise public domain data as an additional category of data for which the controller has flexibility to make its own risk assessment of the appropriate safeguards.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

24. Private sector organisations that need to process sensitive data relating to criminal convictions and related security measures to combat *financial crime* have significant concerns that the Regulation will inhibit their ability to do so. It is imperative that the UK Government press for a more proportionate approach to regulation that recognises the different contexts in which personal data are processed and does not over burden businesses.

25. We welcome the approach proposed by the UK Government as set out the Summary of Responses. However, in addition to the areas identified we urge the Government to:

— Push for clarity that the Regulation will not interfere with organisations' ability to comply with existing international regulation.

— Push for recognition that private sector organisations (that fall outside the scope of the proposed Directive) also have legitimate grounds under the Regulation for processing criminal convictions data to detect or prevent financial crime.

— Seek wider powers for Member States to make common sense derogations from the Regulation in the area of the prevention or detection of crime in the private sector.

— More explicitly recognise the need to take into account the evolving nature of technology, especially recognising that it does not make sense to impose the same international data transfer obligations on data that can be found online in the public domain data as it does on consumer sourced data.

August 2012

Written evidence from the British Bankers' Association

European Union Data Protection Framework Proposals

Please find enclosed the views of the British Bankers' Association to the Justice Select Committee's inquiry into the European Union Data Protection Framework Proposals.

The British Bankers' Association ("BBA") is the leading association for UK banking and financial services representing members on the full range of UK and international banking issues. It represents over 200 banking members active in the UK, which are headquartered in 50 countries and have operations in 180 countries worldwide. All the major banking groups in the UK are members of our association as are large international EU banks, US and Canadian banks operating in the UK as well as a range of other banks from Asia, including China, the Middle East, Africa and South America. The integrated nature of banking means that our members are engaged in activities ranging widely across the financial spectrum from deposit taking

and other more conventional forms of retail and commercial banking to products and services as diverse as trade and project finance, primary and secondary securities trading, insurance, investment banking and wealth management. Members include banks headquartered in the UK, as well as UK subsidiaries and branches of foreign banks—all of which are potentially impacted by this CP.

The proposed EU Data Protection Regulation has critical implications for how BBA members operate. There are a series of key areas in our response where we have provided a justification for amending the impractical, costly and resource intensive burdens, currently under debate. These include:

— Comments on the proposed Regulation and whether it strikes the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them.

— Comments as to whether the UK Government's proposed next steps to take during the negotiations are the right approach.

— Additional next steps the BBA would like the Committee and the UK Government to consider.

1. *Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?*

1.1 Protecting individuals' personal data is an absolute priority for our members. The draft Data Protection Regulation is well-intentioned, but we have some concerns about the unintended consequences.

1.2 This Regulation should strike a balance between providing appropriate protections to individuals without stifling legitimate business activities or creating costs and inefficiencies which are ultimately borne by the consumer. We feel that certain provisions add a layer of bureaucracy that go beyond what is necessary and will not lead to improved protection for individuals.

1.3 Within the current proposal are requirements that do not bring significant benefits to the individual and go far beyond what is requested by financial regulators.

1.4 The proposed Regulation will have immediate cost impact as members will have to change product application forms, front line systems and underlying databases as well as convert existing data held, amend all marketing processes and send new notices to all customers. Additionally, members will need to improve the current processes in place or set up new ones so as to comply with the new law requirements such as—by way of example—those relating to the Data Breach Notification (Articles 31–32), Data Protection Impact Assessment (Article 33) and Documentation (Article 28).

1.5 One bank has estimated that an additional 40 to 80 extra full time employees will be required to enable compliance. One member has estimated that the proposed changes will cost them approximately £50 million.

1.6 The BBA agree with the Information Commissioner's Office in their initial response that, "again there is too much emphasis on mandating the bureaucracy of data protection when the objective of the proposed Regulation is the protection of personal data in practice rather than the creation of paperwork."

1.7 The banking sector is under intense regulatory scrutiny at this time and, aside from the considerations of data protection requirements, is presently deep in discussion regarding the E-privacy directive and national data transparency initiatives such as midata. There is a concern that there are many differing pieces of legislation being introduced without due consideration to where they may conflict and overlap.

2. *Question 2—Will the proposed Directive strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection for police and criminal cooperation in the EU, and on the other for law enforcement authorities to be able to investigate crime without disproportionate financial or administrative burden?*

2.1. The BBA is not providing an answer to your second question as it is not directly applicable to our members.

3. *Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?*

3.1 The UK Government's proposed next steps and BBA comments are below

3.2 *Support the provisions requiring transparency of processing, including the new transparency principle and the requirements for data controllers to provide accessible and easy-to-understand information about processing;*

3.2.1 The BBA supports this proposition as long as it is proportionate and takes into account issues raised in the next section (3.3).

3.3 *Support the requirement for additional information to be provided to data subjects both proactively and in response to subject access requests (subject to consideration of the additional costs), but resist the proposal that subject access rights be exercisable free of charge;*

3.3.1 BBA members believe the Committee and the UK Government must give greater consideration to the appropriateness of many of the requirements for additional information that are unduly burdensome and expensive to provide. These include the following:

3.3.2 *Data request in electronic form (Article 12)*—Data controllers are required to identify individuals making subject access requests, which is unlikely to be possible via some electronic channels, such as email. Banks are open to receipt of electronic requests where practical and secure facilities exist, but we argue that there is no place for this Article in a Regulation whose intention is to remain technology neutral.

3.3.3 In addition, our members have concerns about sending data electronically. Extra controls will need to be implemented so as to ensure that email requests are not fraudulent attempts to obtain information which will require extra resource. The growing IT security issues our members face generally in the fight against fraud is a robust reason as to why this would not be desirable. In addition, the amount of data that could be disclosed may be significant requiring the use of encryption tools that may not be compatible with our customers' IT resources.

3.3.4 *Providing information in an automated manner (Article 12)*—BBA members believe that a requirement to respond to electronic requests in an automated manner has the potential to be burdensome on individuals who will be required to support a secure procedure for the transmission of the data, eg encryption. Our comments on technology neutrality above (3.3.2) apply here equally.

3.3.5 *Timescales for informing the data subject (Article 12)*—Technology has provided for many advances in banking services; however, due to the many numbers of customers (approximately 160 million bank accounts in the UK), and volumes of data, some processes still take time and are challenging to execute. Therefore legislating that subject access requests must be fulfilled within one month (Art 12,2) is a significant challenge and will place excessive burdens on business. We would request that reference to a specific timescale is removed. We also disagree with the ICO's assessment that technology will enable time required to report periods to be reduced.

3.3.6 *Reporting data storage periods (Article 15)*—The proposed Regulations require the specific period for which the personal data will be stored to be relayed to the customer (Art 15,d). We would note that it will be challenging and somewhat cumbersome for the individual to view this information on a privacy notice as different data will have different retention periods. It is difficult to see how specifying a retention period benefits the customer, and provided the business complies with the existing obligations of keeping data on so long as is necessary, then this satisfies the data protection requirements.

3.3.7 *Justification of data processing (Article 14 and 15)*—It is usually very clear to the customer why their data is being processed when contractual terms or legitimate interests are involved. For example, if a customer has applied for a mortgage or bank account then the justification for data processing is apparent. However, the proposed Regulations require specific explanation of the justification for processing to be provided (Art 14, b, Art 15,h). This brings no added benefit to the customer and will lead to confusion; furthermore this is not currently requirement under any financial rules and individuals have not suffered as a result. We suggest the deletion of the following words in Article 14(1)(b) ", including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1)".

3.3.8 Members have similar concerns on Article 15 e,f,g. Businesses should have the choice of signposting customers to this information in their own way and as is appropriate to the circumstances/service etc, be it via a website or other means.

3.3.9 BBA members are concerned about any proposed regulatory change that might encourage spurious and fraudulent requests for information (or "phishing expeditions" as a result of being able to obtain the information free of charge). (Art 12, 4). We therefore agree with this part of the UK Government's proposed next steps.

3.4 *Push for an overhaul of the proposed "right to be forgotten" given the practicalities and costs and the potential for confusion about its scope for both organisations and individuals; however, the Government reaffirms its commitment to the right for individuals to delete their personal data, where this is appropriate;*

3.4.1 The BBA supports this proposition.

3.5 *Resist new bureaucratic and potentially costly burdens on organisations which do not appear to offer greater protection for individuals; examples of this include mandatory data protection impact assessments,*

seeking prior authorisation from the supervisory authority for certain processing operations and the mandatory designation of independent data protection officers;

3.5.1 The BBA supports this proposition.

3.6 *Support the introduction of data breach notifications both to supervisory authorities and affected individuals, but only if the provisions reflect the timescales needed to properly investigate a breach and if a sensible and proportionate threshold is provided which excludes minor and trivial breaches from the scope of the requirement;*

3.6.1 The BBA supports this proposition and the ICO position on this issue.

3.7 *Reaffirm its commitment to a strong and independent supervisory authority at national level and support the establishment of a consistency mechanism to ensure a degree of harmonisation in the application of data protection rules across the EU, whilst allowing independent national authorities some flexibility in how they use their powers;*

3.7.1 The BBA supports proposition.

3.8 *Support a system of administrative penalties for serious breaches of the Regulation's requirements, but push for a more proportionate level of maximum fines, which allows supervisory authorities greater discretion in applying the powers available to them;*

3.8.1 The BBA supports this proposition.

3.8.2 The BBA feels there should be a statutory maximum figure for fines. In addition, there should be further alternative available measures in relation to applying enforcement orders and/or undertakings, as appropriate in each jurisdiction.

3.8.3 Furthermore, the maximum fine of 2% of the annual worldwide turnover is disproportionately high in relation to the risk of harm.

3.8.4. In addition, there are many financial services organisations where the processing of personal data relates to a very small proportion of overall global business, particularly in the investment banking area. It is not fair or appropriate to penalise business operations that are not related to the processing of personal data or which were not associated with the incident other than being a sister company in a shared group of companies. In this respect, fines, if relevant, should be imposed on the basis of the turnover of the legal entity which committed the breach.

3.8.5 As currently proposed, the broad areas where fines can be applied are disproportionate in relation to the risk of harm to an individual that might arise from a breach of the proposed Regulation. We believe it is also unfair to also levy fines against firms for failing to promptly provide personal data in a subject access request (Art79, 4a). Some cases are extremely difficult to provide a return within the current 40 day window (and will be even harder if this is reduced to one month).

3.9 *Push for the removal of many of the powers for the European Commission to make delegated and implementing acts, particularly where these have the potential to make a big difference to fundamental requirements and principles (for example, the legitimate interests upon which data controllers can rely to make their processing lawful or the safeguards that must be established to allow profiling to take place).*

3.9.1 The BBA supports this proposition.

3.10 *Additional next steps the BBA would like the UK Government to include*

3.10.1 We would like the UK Government to support BBA members by making strong reference to the following in the proposed next steps.

3.10.2 *The legality of data processing (Article 6)*—EU law should recognise existing comprehensive financial Regulation.

3.10.2.1 Legitimate interests are one key condition relied upon as the basis for data processing. As currently drafted, the proposed Regulation does not recognise the legitimate interest that businesses have in processing data to comply with extensive domestic financial regulation.

3.10.2.2 Article 6, 1c, states that personal data shall be lawfully processed if it is "necessary for compliance with a *legal obligation* to which the controller is subject."

3.10.2.3 Financial organisations are required to comply with more than *legally obligated* requirements; for instance, there are various Codes of Practice and guidance such as the Joint Money Laundering Steering Group Guidance (approved by HM Treasury), the Financial Action Task Force Money Laundering Guidelines, the guidance on the Payment Services Regulations (approved by the UK FSA), the industry guidance to the Banking Conduct of Business Regulations (approved by the UK FSA) and the International Chamber of Commerce Uniform Code of Practice 600 for trade finance activities. Failure to comply with such rules, guidance and codes of good practice may result in regulatory action and penalties.

3.10.2.4 It is fundamental that the Commission recognises the validity of processing in these circumstances and expands the proposed Regulations to allow data processing in

compliance with any *"Regulatory Rule, Guidance, or industry Code of Practice, either domestically or internationally, to which the data controller is subject."*

3.10.3 *Special categories of personal data (Article 9)*

3.10.3.1 The proposed Regulation includes a prescriptive and rigid set of data categories that can not be processed unless an exemption applies; this creates unnecessary difficulties in practice that do not benefit the individual (Art 9,1).

3.10.3.2 For example, a bank may provide services to a disabled customer; it is preferable for the bank to record this information so that staff can be sensitive to the specific needs of the customer. However, as this is not core business data for a bank, the proposed Regulations would require the bank to ask the customer for their consent to record this information. This is clearly unnecessary and may upset the customer. Sensitivity is also dependant on the context within which it is used ie ethnicity or disability is not sensitive unless used for discriminatory purposes.

3.10.3.3 A better outcome would be derived from not having a defined subset of personal data but by having one combined list of conditions for processing all personal data. If this is not possible, then we would like two exclusion conditions to allow processing of data when it does not adversely impact the rights, freedoms and privacy of the individual.

3.10.4 *Combating fraud concerns (Article 6, 9, 20)*

3.10.4.1 Banks are required to collect, assess and retain various types of data relating to preventing and combating fraud and and other criminal activities such as anti-money laundering and terrorist financing. This data collection is relevant both prior to and as part of internal and external investigations. It is not appropriate, as is currently implied in the proposed Regulation, to limit the legal obligations around storing such data (Art 6 and 9).

3.10.4.2 Therefore the BBA believes the Committee and the Government should consider an exclusion in Article 9 for processing that is necessary for compliance with a legal obligation, a regulatory rule or a piece of guidance, industry code of practice to which the controller is subject.

3.10.4.3 An additional processing condition is needed in Article 6 to explicitly allow certain anti-money laundering and fraud detection purposes. This processing is necessary to protect customers and businesses from financial loss and for regulatory reasons. This provision could be similar to the wording under Section 29 of the UK Data Protection Act.

August 2012

Written evidence from the Market Research Society

EU DATA PROTECTION FRAMEWORK PROPOSALS

Introduction

1. With members in more than 60 countries, The Market Research Society (MRS) is the world's largest research association. It's for everyone with professional equity in market, social and opinion research and in business intelligence, market analysis, customer insight and consultancy. In consultation with its individual members and Company Partners, MRS supports best practice by setting and enforcing industry standards. The commitment to uphold the MRS Code of Conduct is supported by the Codeline service and a wide range of specialist guidelines.

Response to Terms of Reference question

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

Overview

2. MRS is generally supportive of the current proposal for a General Data Protection Regulation and of the next steps the UK Government proposes to take during the negotiations. We do however have specific concerns about provisions relating to consent, protection of personal data of children, profiling, business burdens created by the proposals and provisions relating to historical statistical and scientific research.

Consent

3. The first principle of the MRS Code of Conduct is:

— Researchers shall ensure that participation in their activities is based on voluntary informed consent.

4. Therefore researchers rely heavily on consent as the basis for fair and lawful processing. Much of that consent is very clear—where a researcher invites a data subject to participate and they agree to do so or where a direct question is asked and an answer is spontaneously and voluntarily given.

5. In some cases researchers may rely on the second data principle to process data to invite data subjects to participate in a research project. For example, in the case of customer satisfaction research, an individual whose data has been collected in order to obtain a product or service may be invited to give their views on the quality of service they have received. It has been accepted by the Information Commissioner's office that processing data in this way (ie inviting them to participate in research) is not incompatible with the purposes for which the data was collected (provision of a product or service).

6. A number of major social research projects also rely on the ability to contact individuals whose data may have originally been collected for non-research purposes. Examples of this include:

- Victims of Crime surveys, conducted for the Home Office or for local police forces; and
- The GP-Patient Survey for the Department of Health, which interviews patients who have visited their GP in the preceding six months.

7. There are a significant number of European market, social and opinion research projects, aimed at improving society within Europe, where there is a need to be able to gather representative views from European citizens. This is achieved by being able to contact any European citizen on a random basis. If the ability to do this is diminished by legislative actions that are likely to exclude consumers and citizens from taking part, it will dilute the statistical reliability of results for understanding both social and commercial issues. This would be highly damaging for UK and European policy makers and businesses.

8. The current proposal defines the data subject's consent as:

> *any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;*

9. This appears to be an evolution of the definition rather than a radical change. However this is dependent upon the definition and interpretation of the phrase "by a statement or by a clear affirmative action". Any definitions within the revised legislation, whether existing or new, should not contain any ambiguity. The current definition for consent is ambiguous. In the past, regulators in Member States such as Germany have defined explicit consent as written consent. It is essential that if the definition of consent is to be amended it does not require written consent. This would seriously undermine the use of current and future technologies for data collection, which are widely used for research purposes.

10. In research a respondent to a research project provides the answers to the questions they are asked, having been informed of the identity of the researcher, the purpose of the interview, and of their right to withdraw at any time. There is not always a specific question to obtain permission for the processing of data, but the freely given, specific, and informed consent of the data subject is explicit nonetheless from the data subject's willingness to answer questions posed by the researcher. We believe is it essential that any requirement for explicit consent retain the possibility of it being signified by statement or action by the data subject.

Protection of personal data of children

11. Although neither the 1995 Directive nor the 1998 Act explicitly contain provisions for the protection of children, MRS has always recognised that children and young people are vulnerable members of society and the MRS Code of Conduct contains a number of specific rules to offer children additional protection. For example, the consent of a parent or a responsible adult acting in the place of a parent is required before a research interview can be conducted with a person under the age of 16. Separate MRS children's guidelines also prohibit research with minors on products that are illegal for the age group, and set out additional criteria which should be followed to provide maximum protection for respondents that are under 16.

12. It should also be noted that there are circumstances where the asking of parental consent may harm or adversely affect children, for example, research with users of helpline services such as Childline. The MRS Code of Conduct makes provisions for this by the waiving of parental consent requirements in limited circumstance subject to ethical review and approval of the MRS Market Research Standards Board.

13. MRS, by having specific rules governing research with children, recognises that children and young people are valuable members of society and have the right to participate in society, including participating in research projects relevant to them, whilst offering adequate protection via the MRS Code of Conduct, a robust ethical research framework. We believe this is *balanced approach* which protects children whilst also respecting that they have views which need to be heard as children wish to be able to determine their future society. If it is decided that additional provisions relating to children are required, the Regulation should take an equally balanced approach.

14. The current proposal defines a child as a person under the age of 18, in line with the UN Convention on the Rights of the Child, but the only substantive provision relating to children is in Article 8:

> *For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.*

15. Persons under 18 may leave school, marry, join the Armed Forces or attend university and are autonomous persons. MRS recommends that if additional restrictions were to be introduced that these mirror the self-regulatory rules already in place in Europe, the majority of which require consent of a parent or responsible adult acting in the place of a parent with *under 14s*. Consideration should also be given to situations where parents or guardians are not engaged in the children's lives and where obtaining consent may cause harm or detriment to the interests of the child. As explained above the MRS Code of Conduct requires such consent before interviewing persons under the age of 16.

16. It is the view of MRS that if society is to properly prepare children and young people for the transition from childhood to adulthood that the transition should start at 16 at the latest, not 18.

Profiling

17. The proposed regulation in Article 20 defines profiling as:

(a) a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to valuate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

18. MRS welcomes that this definition is limited to measures which produce "legal effects" or "significantly affects" the individual. A broader definition (such as that used by the Council of Europe in its Recommendation 2010(13))[30] would encompass many statistical processes (such as sampling) used by research. This could have a huge and detrimental impact on the quality and representativeness of research samples and research results. For research to be robust for evidence based policy making, an important facet of European policy development, plus for broader commercial uses such as business development within Europe, it is essential that researchers are able to classify potential respondents to ensure that representative samples can be drawn. The introduction of a very broad definition could have unforeseen impacts on significant research projects such as Eurobarometer and the Labour Force survey, which are widely used for policy development within Europe.

Business burdens created by the proposals

19. MRS notes that the Commission estimates that businesses in the EU will save up to €2.3 billon by their proposals. However, these benefits would appear to be outweighed by a number of additional obligations and requirements being proposed including the appointment of data protection officers (DPO).

20. Given the detailed responsibilities of the DPO set out in Article 38 of the proposed regulation[31], it would not be possible to pool the responsibility of a group of companies under a single officer, meaning that multiple appointments would have to be made. Further the proposal contains additional requirements to conduct privacy impact assessments for all material data processing events and products. While it is difficult to estimate the exact costs of these requirements, for a large research organisation they could easily add over £5 million annually to the cost of doing business. The additional process steps and delays that would take a toll on business performance are not included in this figure.

21. While the independent DPO model is one method of ensuring accountability, as an alternative consideration should also be given the concept of a Chief Privacy Officer who is an integral part of the management of a business and would have overarching responsibility for all data protection and privacy matters in an organisation or group of organisations.

Historical, Scientific and Statistical Research

22. The Commission's proposals contain a number of provisions relating to historical statistical and scientific research. These build on existing provisions in the 1995 Directive and the 1998 Act and are essential for our sector and we strongly urge that they be retained in any final text. These include:

- Personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes (Article 5e).
- Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful (Article 6.2).
- The prohibition on the processing of special categories of personal data shall not apply where processing is necessary for historical, statistical or scientific research purposes (Article 9.2i).

[30] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling

[31] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

— Data held for historical, statistical or scientific research purposes is exempt from the right to be forgotten (Article 17.3c).

Conclusion

23. Data protection is a key facet of the business of market, social and opinion research. MRS supports the development of a coherent, harmonised and proportionate framework for this area. We wish to remain closely involved in the process and would welcome further opportunities to comment on the proposed legislation, during its passage through the European Parliament and Council of Ministers.

August 2012

Written evidence from ISBA

EUROPEAN COMMISSION'S DATA PROTECTION FRAMEWORK PROPOSALS

About ISBA

ISBA—the Voice of British Advertisers, is the representative body for UK advertisers. We have in excess of 400 members representing business, not for profit and the public sector. Collectively ISBA members account for more than £10 billion of media spending.

Summary

— We welcome an update to the EU law. Digital technology is changing fast; citizens and consumers need to feel comfortable about the use of their data, just as advertisers also need to be assured that their use of data respects the rights of the individual.

— European data protection legislative framework should remain high level. The Commission's focus should be on inconsistencies of application and enforcement across the EU. There is a danger that attempts to legislate for the current digital age will become rapidly out of date. ISBA supports a principles-based legal regime that can evolve as technologies develop.

— This submission relates only to the Regulation for general and commercial data protection. Our members believe that this draft Regulation presents a serious threat to the advertising sector and, while accepting that the parallel Directive is an important legislative area, would like to ensure that the enormous impact that the draft Regulation could have on our sector is recognised by the Committee.

— The obvious advantage of a Regulation rather than a Directive is the enforced harmonisation of standards throughout the EU. However, this also presents a significant risk that the final text will reflect the most restrictive laws currently in place in a Member State and/or be the result of clause bargaining at the last moment, leaving business to implement laws whose meaning is not clear.

— Our concerns about the proposals from the EU are centred on the aspects that will act as impediments to the development of digital media and marketing opportunities. We include real life anecdotal evidence/practical consequences/day-to-day examples of the proposals' possible effects.

Response to Terms of Reference Questions

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

1. We welcome the Inquiry's Terms of Reference, which recognise the need to strike a fair balance between the rights of the individual to ensure that their personal data is protected and the rights of businesses to engage with consumers. In the current draft Regulation that balance is unfair, and ultimately places unreasonable (and to some extent impossible) requirements upon businesses.

2. The draft Regulation appears to lead to a regulatory regime that would make business operations more expensive and difficult. This could potentially undermine entire advertising businesses and the businesses that advertising supports and drives, ultimately inevitably impinging on employment, growth and innovation in the economy. ISBA is working with its members and the industry to develop figures showing the potential impact of the proposals to the Regulation. Research undertaken by the Future Foundation and commissioned by the Direct Marketing Association confirms that it could cost the UK direct marketing industry up to £47 billion if the EU Data Protection Directive Proposals are not amended. http://www.dma.org.uk/

3. Given this is just one part of the broad advertising eco-system, the cost for our industry could be extremely high.

4. We support laws that work to protect consumers' personal data and we believe that updating the current law on data protection in light of the progress in digital technology is sensible. However, we do not think that the proposed EU-wide Regulation in its current form is an effective way to address this need.

5. ISBA is seriously concerned about the content of the draft Regulation which we believe could significantly burden businesses and hinder growth in the advertising industry, in particular the direct marketing and digital sectors. We reject the European Commission's premise that it will lead to a net saving for companies estimated at €2.3 billion and call on the Commission to provide a clearer evidence base that shows where these savings may come from and also recognises the costs to businesses from the new measures that they are proposing.

6. Our assessment is that the Regulation could stifle innovation and increase costs, thus nullifying any potential economic benefits to businesses. We recognise that businesses benefit from more consistent rules across Europe, but question how realistic the draft Regulation's ambition (to lead to laws being genuinely consistent across all member states) is.

7. ISBA believes that the European data protection legislative framework should remain high level, with the Commission focussing on inconsistencies of application and enforcement across the EU. The Commission's attempts to legislate for the current digital age are likely to be quickly out of date, and we encourage the Commission to focus on a principles-based legal regime that can evolve as technologies develop.

8. The Commission must recognise that consumers benefit from a principles-based legal regime which ensures people's data is protected, while still giving them the benefits from the services and goods supplied to them through the data-driven economy.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

9. We are pleased that the UK Government recognises the threat that this Regulation poses to industry, and welcome the recognition of the advertising industry's concerns about the Regulation in the Government's response to the "Call for Evidence" submissions.

10. Naturally, we do not know the detail of the UK Government's focus in Council negotiations, but our understanding is that they are taking a proportionate approach, which is one we support. This approach is also evidenced by their next steps as set out in the Summary of Responses document, and in general these are next steps that we support.

11. In particular, those areas raised by Government which ISBA members have concerns about are:

— increased bureaucracy and business costs;

— the workability of the "right of be forgotten"; and

— the excessive number of implementing acts.

12. The advertising industry would be severely impacted by the bureaucracy and sanctions that are required in the draft Regulation. Most of our members are larger organisations; it is worth noting, however, that meeting the requirements in the Regulation will be more difficult for SMEs.

13. These potential burdens include: Hiring a Data Protection Officer, addressing the fact that organisations could be liable to a fine of 2% of their annual turnover, and processing the increased amount of data now classified as "personal". The Commission speaks of €2.3 billion savings for business. ISBA disputes the idea that money will be saved, and strongly believes that it will impose massive costs on businesses.

14. Additionally, UK companies benefit from a strong and effective Data Protection Authority in the Information Commissioner's Office (ICO), and we are also concerned that the increased bureaucracy that the draft Regulation imposes on the ICO will undermine their ability to act as an effective enforcement body. We would like to see a Regulation that enables the ICO to continue to be effective through being independent, as well as being able to make decisions based on genuine risk.

15. Evidence from our members confirming the bureaucratic and financial burden on businesses if the Data Protection Directive proposals are not amended is as follows:

— Lose the ability to directly track users would lead to loss of budget for online acquisition.

— Lack of management information would remove the use of aggregators on a cost-per-sale basis.

— Relatively expensive generic search terms can only be justified via optimisation and attribution modelling, which would be badly affected by these proposals.

— The online model could be destroyed, forcing a reduced digital spend.

— Loss of cookie based targeting functionality would effectively put large parts of the display media ecosystem out of business (ie ad networks, trading desks, data brokers, DSPs, SSPs and ad servers).

— Users' personalisation of content would suffer. The inability to track a user's behaviour online means that they would be served a less personalised experience. Remembering a user's history or shopping basket is something that online consumers have come to expect, forming part of the online shopping experience. Without this, the evolution of online shopping/browsing would be badly affected.

— Targeted marketing would be very difficult to achieve, resulting in a "scatter-gun" approach. Many consumers want advertisements that are relevant to them. A lack of a means to create audience segments will result in less targeted and relevant messages.

— IP targeting can prevent ads being shown in the wrong country and/or region. Without this, there is no guarantee that ads were served in the right region. For a consumer this also results in irrelevant advertising.

— Affiliate or performance-based marketing, outside of driving call centre traffic or store footfall, would also disappear over time without the use of cookies.

— Further complexity to the Search Engine Optimisation (SEO) landscape is threatened. If this data proposal interrupts the consumer experience and acts as a deterrent for consumers from using digital, this will threaten to scupper the social search focus SEO's currently have.

— There may be a negative impact on mobile/smartphone usage as, outside the web experience, messaging services/apps from "WhatsApp" (a cross-platform mobile messaging app for iPhone, Blackberry, Android, Windows phone and Nokia) to Skype will be subject to similar issues.

— It would also be incredibly hard to justify online marketing budgets for digital display, as performance would be severely affected due to the inability to serve content based on a user's interests. This is another example of providing the user with a worse overall online experience. Therefore we could destroy a progressive online industry by stunting the evolution of the digital age.

The introduction of a "right to be forgotten"

16. There are aspects of the proposed "right to be forgotten" that will be attractive to users. Great care needs to be taken to avoid making legislative promises that the global structure of the internet makes it impossible for government and business to implement. We may all suffer from reputational damage. From a strictly advertising industry perspective the right to be forgotten presents a considerable difficulty. The impact is mainly on direct marketing and third party data list brokers.

17. The current data protection laws already set out rules that provide individuals with information on the identity of the organisation processing their personal data, and the purposes of this.

18. The EU rules currently provide individuals with information on both the identity of the organisation processing their personal data, and the purposes of this. Articles 12 and 14 of the current Directive provide a right of access and a right of objection. Individuals can require their personal data to be erased, blocked, changed or deleted.

19. The proposed Regulation would require companies that hold an individual's data and pass it to third parties to not only have to delete their information, but also to ensure that the third party deletes this information too. This would be burdensome for both businesses and the police.

20. The introduction of the phrase of a "right to be forgotten" sets unrealistic expectations for the consumer as to what is achievable. It is often simply impossible for data on the internet to genuinely be "forgotten" as this data may be shared by a number of "parties" out of the control of the original data processor. Although there is certainly a need to provide greater information to individuals about their rights to erase data, creating unrealistic consumer expectations is not a worthwhile exercise.

The extension of powers to the Commission through "delegated" and "implementing acts"

21. The Regulation makes provision for the extension of Commission powers through "delegated" and "implementing acts". The ability to avoid further legislative oversight by the European Parliament and Member State Parliaments is a matter of concern for business.

22. The Commission has included many of these acts which enable it to eventually amend the Regulation without any proper industry consultation, or checks and balances of an orderly legislative process via parliamentary scrutiny. This leads to increased business uncertainty about the future shape of data protection law in Europe. Furthermore, the lack of proper consultation with industry is extremely worrying and will continue to deepen the problematic issues around the democratic accountability of the Commission.

The definition of personal data (eg including some IP addresses & cookies as personal data) and consequences for profiling

23. In addition to those areas raised by the Government in their document, ISBA has particular concerns about the impact on the advertising sector by extending the definition of personal data and by mandating unworkable consent requirements.

24. The proposal redefines the concept as "any information relating to a data subject"—consequently some IP addresses & cookies will become "personal data". However, IP addresses and cookies are nearly always anonymous data; this new Regulation would unnecessarily personalise these data sets with severe consequences for responsible and useful profiling.

25. Cookies and IP addresses are essential tools for advertisers to target advertising, ensuring that ad content is relevant to individual browsers. Targeting or behavioural advertising does not use personally identifiable data.

26. Confusing these data sets with truly identifiable personal data is bad practice. It will mislead individuals, restrict the ability of all internet users to communicate and add costly red tape to business practices.

27. In proposing a blunt catch-all definition of personal data, the Regulation proposes that some cookie data and IP address data should be considered "personal". ISBA believes that this is an unreasonable approach, as in many cases IP addresses and cookies are not directly linked to an individual. The new Regulation makes no distinction between this type of data (which is not directly identifiable) and directly identifiable information (eg full postal address). The use of cookies and IP addresses is essential to the smooth running of the internet. It is also necessary for the delivery of targeted advertising that is relevant to a browser but that uses no directly identifiable data.

28. The personalisation of these data sets could be very damaging, particularly if the consent requirements are interpreted to require explicit consent for the processing of cookie data. Furthermore, the impact on users of having what is currently "anonymous" data, like cookie data, considered "personal" could undermine the way in which clearly identifiable personal data is processed. Businesses will be forced to treat these data sets equally, being subsequently overwhelmed with vast quantities of data.

29. ISBA calls for the UK Government to advocate a risk-based approach that addresses the issue of personal data based on the likelihood of identification of an individual, rather than a blunt catch-all definition. This more granular approach has been advocated in the Information Commissioner's Office's code of practice on Personal Information Online.

30. Developing this concept further, ISBA believes that both business and consumers would benefit from an approach that considers recognising a third category of data, which is neither directly identifiable nor completely anonymous. Rules should be created for the processing of such data, but they should be proportionate and not as onerous as the rules that are required for processing of directly identifiable personal data.

The requirement for explicit and informed consent for data collection & processing

31. As raised above, any moves to require "explicit" consent for processing of cookie or IP data should be avoided. This would lead to increased "opt-in" mechanisms for the collection of what are effectively anonymous data sets. Businesses would essentially be forced to personalise these data sets in order to obtain the explicit consent of users. This would prove to be hugely burdensome for businesses and would severely undermine the consumer's online and offline experiences. From a practical point of view, it would lead to multiple pop-ups online for cookies and would hugely affect the direct marketing industry, with the likely impact being an increase in unaddressed mail.

32. Taking the cookies issue specifically, industry is working hard to comply with the consent requirements set out in the ePrivacy Directive, and so amending the consent requirements in this Regulation would further increase burdens. Therefore, it is critical that (as per Article 6 1. f in the draft Regulation), the processing of personal data can be lawful "if this is necessary for the purposes of the legitimate interests pursued by a controller". We accept that such interests can be overridden by the rights and freedoms of the data subject, in particular where the data subject is a child*. Any moves to require explicit consent for the processing of categories of data that are unique to a device—like cookies—but that do not directly identify an individual, would be severely detrimental to the UK economy.

33. *The definition of a child is redefined as anyone under 18. It remains a puzzle that anyone would think it at all practical to enforce this against people aged 17 ¾. "Verifiable" parental consent is required collecting data from children under 13; again this is a difficult concept to enforce in a digital environment where the (perhaps misguided) intentions of a child can be visited on the website provider.

August 2012

Written evidence from Symantec

EUROPEAN UNION DATA PROTECTION FRAMEWORK PROPOSALS

1. Symantec's welcomes the opportunity to provide input to the Justice Committee enquiry given our role as the global leader in providing technologies that protect the world's information and empower individuals to secure and manage their personal information and identity online. Our technologies help companies to apply data protection every day in a practical manner by managing their systems, securing their customers' data and ensuring data protection compliance.

2. The following response to the Committee's questions will be focused on the proposed Regulation only. However, many of the points below relate to concepts and terms that are mirrored in the proposed Directive and therefore will also be relevant to the Committee's wider discussions.

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

3. The review of the EU Data Protection Directive (95/45/EC) is seen by Symantec as a welcomed opportunity to consider whether the legal framework in place in the UK since 1998 is still relevant and

appropriate . Particularly given that increasing amounts of information is transmitted, processed, shared and stored across electronic networks, not only in the EU but around the world, at the click of a button. This new era brings opportunities as well as challenges for the privacy and security of data that must be addressed to ensure citizens information is secured particularly given information is a key target for cyber criminals according to Symantec's latest Internet Security Threat report.[32]

4. The proposed Regulation was welcomed by Symantec as a step forward in achieving a more harmonised legal framework that enables greater clarity and certainty on how European data protection laws should apply to individuals and be applied by businesses, particularly those organisations operating across Member States. Significant changes are being proposed that have the opportunity to introduce positives changes that will be felt by businesses and citizens like. For example the moves to introduce a country of origin approach based around a lead supervisory authority and a sector wider data breach notification requirement. However, for Symantec a key objective of the review is finding the right balance that ensures individual's right to privacy is protected while also enabling businesses to process data needed for legitimate purpose such as providing online goods and services that EU citizens may in fact want and need (such as online security). In many areas this balance is found such as the requirements for security measures to be place that are based an analysis of the risks to the data being processed. However, there are also areas where proposals being made are overly prescriptive and could introduce barriers to organisations ability to process data which could reduce the level of data protection that UK citizens currently enjoy. An area where this is of particular concern is the proposed changes to the definition of personal data.

5. The proposed Regulation (Article 4.1) expands the definition of personal data to include any information that may be related to a data subject including online identifiers such as cookies and IP addresses. If introduced in its current form Article 4 would effectively means that sectors which need to process data, but may not be in a position to attribute that data to a specific data subject, could be compromised. This is because all data would be classed, first and foremost, as personal data because it may be able to be used by anyone to identify an individual at some point.

6. It is unfortunate that the importance of the context in which data is being processed as to whether identification of data subject is even possible is not recognised. For example the computer security industry may process IP addresses to prevent online attacks and protect EU citizens and organisations like banks, hospitals and schools. These IP addresses are processed as traffic data and therefore cannot be attributed to a specific individual by the security company but are vital data to process in order to protect online users from cyber threats such as a hacking or spam attack. Clearly overall the proposed Regulation is looking to increase and not reduce the level of online protection of EU citizens. However, it must not take steps that introduce barriers that could prevent, or stifle those needing to process data in particular circumstances or contexts, such as processing strictly necessary for information security purposes. The Regulation outlines the importance of being able to process data strictly necessary to protect network and system from malicious actions that could compromise the availability, integrity, authenticity and confidentially of data stored and transmitted through these networks (Recital 39). Given the importance of ensuring the computer security industry is able to process data necessary to prevent online attacks, the current wording of Recital 39 should be made more prominent in the Regulation itself.

7. In light of the fundamental importance and implications of the changes proposed to the definition of personal data Symantec would welcome the UK government taking a lead in the EU discussions on this issue.

8. The proposed Regulation should also not introduce changes that could introduction barriers to the further development and deployment of innovative business models such as cloud computing particularly given the impact this could have on the development of EU companies, including the UK based Symantec. Cloud (formally MessageLabs).

9. For example, the proposed Regulation calls for data processors to seek "prior permission" from a data controller before using another processor. This means that data processors should gain prior authorization from controllers when wanting to use a sub-processor. Data processor may use a large number of sub-processors in their operations at different points of the processing. In a cloud computing environment multiple sub-processors may be used to process different elements of data that need to all be available simultaneously for the business model to be effective A requirement to have prior permission before using a sub-processor could not only introduce a significant compliance burden on processors but more importantly would lead to data processing being disrupted while authorization is gained to use a certain sub-processor. Introducing a requirement that could potentially stop data flowing between data processors because authorisation is needed from a data controller, who may be in a different country and perhaps a different time zone, could have a serious impact on the ability of UK based companies to meet EU customer's requirements and could directly impact data subjects access to data. It would also introduce another administrative requirement that would mean additional costs that would have to be met by both data controllers and processors and could ultimately even be put through to data subjects. Symantec believes that where there are aspects of the proposed Regulation where current contractual agreements between controllers and processors have proven to be effective and where changes could significantly disrupt the further development and availability of cloud computing in Europe these should be raised by the UK government in its negotiations.

[32] Symantec Internet Security Threat Report 2011 http://www.symantec.com/threatreport/

10. Overall Symantec remains supportive of the current Directive's hierarchy and definitions of data controller and data processor which remains appropriate and well understood by industry. There is a concern however that proposed changes, such as the extension of liability for a breaches of the Regulation to both data controllers and data processors or the introduction of the concept of joint data controllers, could create an imbalance in the legal framework and result in legal uncertainty over who is ultimately responsible for personal data. The current legal framework makes it clear that it is the data controller that is ultimately responsible. Given that this is fully understood it is felt that this approach should remain unchanged.

11. Finally Symantec support the concerns raised by the UK government regarding the use of delegated acts, particularly related to the lawful business processing of data (Article 6), The introduction of delegated acts that could lead to sector specific requirements would put at risk a core aim of the review itself; the introduction of a single, harmonised data protection system across the EU. However, Symantec would also like to highlight specific concerns that the use of delegated acts is a direct challenge to the principle of technology neutrality and is a move that could lead to the introduction of technological requirements.

12. For example the Commission is given delegated powers to specify design requirements for how privacy by default and design is to be implemented. This would result in the introduction of technology mandates in a legal framework that is supposedly technology neutral. In Symantec's view Privacy by Design and Privacy by Default should be introduced into the legal framework as a process and not a technology mandate. To ensure this the delegated powers in this area should be removed. In the area of data portability the proposal that the Commission should be able to specify the "electronic format" and the technical procedures and standards that should be used for data portability would effectively mean that the measures developed by the market and the investment already made by industry in this area could potentially become worthless. A situation where industry would be required to remove proven and effective technological formats and solutions where there is no proven market failure and replace this with a Commission developed "electronic format" would result in significant administrative burdens and cost implications for industry and more importantly could lead to possible disruption for users.

13. Symantec believes that the areas where delegated powers would lead to the introduction of technological specific requirements or mandates should be raised by the UK government in its negotiations strategy as a priority area for deletion in order to maintain the technology neutrality of the legal framework that must be able to stand the test of time just as the 1995 Directive has.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

14. Symantec welcomed the UK governments response to its call for evidence and believe the Ministry of Justice should also be recognised for their willingness to engage with stakeholders throughout the consultation period.

15. Overall for Symantec the key issues identified in the response as forming the basis of the UK negotiations are considered appropriate and relevant and are generally supported. In particular Symantec supports the UK Government's call for the reconsideration of the delegated powers given to the European Commission through the Regulation given the concerns raised above. We would call on the government to prioritise the removal of delegated act that would introduce technological mandates to maintain the technology neutrality of the future legal framework.

16. Symantec also welcomes the government's support for the introduction of data breach notification which is seen as a key tool for increasing citizens transparency and understanding regarding their information. However, in light of the proposed Regulation's aim to ensure harmonisation of EU law Symantec believe that any sector wide breach requirements should reflect what has already been enacted into EU law under the revised ePrivacy Directive (2009/136). For example, the requirement to notify a breach within twenty four hours is seen as a step too far and could mean that an organisation impacted by a breach may find themselves focusing more on meeting a notification deadline, due to the threat of a sanction if this deadline is not met, at a time when the priority should be taking steps to address the breach and minimise possible impact and risks to data subjects information. It is also suggested that the introduction of a "threshold" criteria based on the harm likely to be caused by a breach for determining the level at which a breach would be serious enough to trigger notification should be highlighted in discussions. This would also address concerns relating to over notification of any and all breaches to authorities and citizens and given this approach is within the ePrivacy Directive it would help to put in place a single, harmonised and also appropriate and workable data breach notification regime applicable for all sectors across Europe.

17. Also Symantec shares the UK government's support for data subject access requests as an important concept that empowers individuals by increasing transparency of how data is being used. The concern raised over the proposed introduction of a free of charge rights of data access are also understood given the possible negative impact that unnecessary requests or disproportionate requests could have on businesses which must allocate resources and trained staff to respond to requests. Given the amount of information, particularly electronic communications, that could be involved in a subject access request the Regulation should recognise and reflect the effort that could be involved in a data subject access requests. For example an organisation presented with a data subject access request could spend considerable time reviewing numerous documents to

delete personal data related to other data subjects in order to protect the privacy of their personal data. This time and effort involved in responding to data subject access requests that now involve all types of data should be reflected in any exemption to ensure the volume of data that may be involved in a data subject access request is taken into consideration when assessing a request.

18. The call for an "overhaul" of the introduction of a Right to be Forgotten is also welcomed given that it is still not clear whether what is being suggested in Article 17 of the Regulation will actually achieve what is being intended. Symantec would support a requirement for data controllers to erasure data that exists within its perimeter, for example on servers that the controller effectively controls. However, Article 17 should make it clear that a data controller's responsibility to delete data should only extend to the data held with the data controllers own perimeter and therefore control. Given that the administrative sanction for not complying with Article 17 is a fine of up to 250,000 Euros or up to 0.5% of an enterprise annual worldwide turnover, there is a need to ensure that the requirements placed on data controllers are those that a controller has within its powers and authority to comply with.

19. However, as highlighted above given the importance of the definitions proposed in Article 4 and the impact the changes proposed will have to subsequent requirements throughout the Regulation (such as consent) Symantec would like to suggest that the UK government include the definition of personal data as an additional area to be covered in their negotiation going forward.

20. Also while Symantec agrees that a significant part of having an effective legal and regulatory framework is having an effective enforcement structure backed up with appropriate and meaningful sanctions, there are still concerns that the basis for how fines could be issued are actions taken intentionally or negligently without any single and harmonised definition of negligence. Also the lack of any graduation in the proposed penalties structure is questioned and does not take into consideration the seriousness of a breach of the Regulation. This could result in a situation where a significant fine is imposed for an incident regardless of the impact or likely or real harm to data subjects and therefore warrants consideration in the UK government's discussions.

21. Also as highlighted above Symantec supports the proposed changes to achieve clarity on applicable law based on a lead supervisory authority. However to ensure this approach is successful it is important to ensure consistency of this approach throughout the Regulation. Therefore the Regulation should make it clear that it is the lead competent supervisory authority that is able to impose penalties. Without this clarification organisation operating across Member States that commit minor breaches of the Regulation could find themselves fined by multiple authorities. Given the current financial levels of the sanctions this could mean that EU businesses may find themselves simply put out of business for what may be minor offences under the current Directive's regime.

22. This need to ensure consistency of the lead supervisory authority approach throughout the Regulation also needs to be recognised in the UK negotiation position related to the role of DPAs. The UK's support for the independence of DPA's is supported by Symantec as are the proposal in the Regulation to introduce greater consistency and mutual recognition between data protection authorities. However, there are some concerns as to the possible impact of the call for national authorities to still have "some flexibility" in how they use their powers.

23. For the lead supervisory authority approach to become a reality and the clarity needed on applicable law to be achieved the lead authority, or "one stop shop" structure is key. At the moment the reality is that many of the Regulation's articles as currently drafted could undermine the very notion of a lead authority and put at risk the measures taken to achieve harmonisation on applicable law. For example Article 52 states that an authority can conduct an investigation on its "own initiative" on the basis of a complaint. This could result in organizations not knowing from one day to another whether they would be required to comply with only the requirements of their lead authority or also every other authority that may be conducting their own investigation. Calling for national authorities to have flexible, rather than calling for amendments to ensure consistency of the lead authority model, could undermine the efforts made in the Regulation to achieve the clarity on applicable law that has been a core aim of the overall review.

24. The UK Government's negotiation position calling for the reduction of burdens and bureaucracy for businesses is of course supported. But the reality is that the introduction of a transparency principle and moves to include accountability into the legal framework will increase the information requirements on businesses. It is not clear what affect the accumulative compliance burden and related costs this will have on organizations. When combined with the additional administrative and information requirements in the area of international data transfers, privacy by design, data portability, as well as the as yet unclear privacy impact assessments and prior authorization requirements from DPAs. Symantec has concerns about the possible effect on our operational efficiency and the ability to do business in Europe if all the administrative and information requirements are introduced. Particularly as there does not appear to be any recognition given to, or benefits offered to, responsible organizations that can demonstrate they have met all of the requirements being proposed. In light of what will be involved in complying with a transparency principle the UK government is urged to include in its negotiation strategy calls for the legal framework, perhaps through the enforcement structure, to recognise and take into consideration the organisational steps and investment made to comply with the

transparency principle by accountable organisations and offer suitable benefits for organisations that can demonstrate they are compliant and accountable.

August 2012

About Symantec

Symantec is a world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. Further information can be found at www.symantec.com. Symantec appreciates this opportunity to submit comments to the Justice Select Committee. For further information, please contact Susan Daley, Manager of Government Affairs, UK & Ireland, Symantec, 88 Wood Street, London, EC2V 7QT tel-07809 492 490 susan_daley@symnatec.com

---

Written evidence from the Business Software Alliance

EUROPEAN UNION DATA PROTECTION FRAMEWORK PROPOSALS

The Business Software Alliance (BSA)[33] is the leading global organization dedicated to promoting a safe and legal digital world. We are grateful for the opportunity to provide input to the UK Parliament's House of Commons Justice Select Committee call for evidence on the European Union Data Protection Framework Proposal. Our comments in this submission only reflect our views on the proposed *EU Data Protection Regulation* and as such would like to address the question as to whether;

> *"The proposed Regulation strikes the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?"*

BSA companies deliver a range of digital products and services to consumers across the EU. For our members, data protection is an essential concern and a top priority when developing and marketing products and services with privacy relevance. We therefore believe that a modern legal framework should:

- Be based on a *balanced and proportionate approach* that ensures data is protected and secure and can help citizens better understand and control how their data is processed, give regulators a tool that can grow and evolve with the technology it aims to govern, and provide data controllers and processors with the legal certainty they need to develop new services;
- Provide *workable solutions for real needs that can be implemented* in practice, accurately reflect citizens' expectations and remain technology neutral;
- Be based on a *context and risk based approach to privacy* and avoid blanket rules to data protection that ignore the broad variety of possible contexts and purposes of data collection and processing;
- Ensure a *properly functioning internal market for the free flow of data, with a harmonized level of personal data protection* that provides legal certainty and consistency for both businesses and consumers;
- Be *technology neutrality.* The rules need to recognise and take into account the fast evolving technological environment, consumer and social behaviours and norms, as well as the use of the Internet;
- *Preserve the ability to provide for the security in the online world* by allowing security technologies to continue to be developed and deployed to mitigate identified risks; and
- Reflect our *global networked society*, by ensuring efficient and seamless *international data transfers*.

A Framework that does not provide the right level of balance, legal certainty and does not address the nature of today's global business and technology could significantly dampen the further development of the digital economy:

- By raising the compliance costs and restricting the flow of data, thus threatening the efficiency and productively gains provided by ICT based solutions such as cloud computing; and
- By dampening growth and investment in the digital economy and stifling R&D and the development of new business models, products and services

A Balanced Approach

BSA would welcome enhancements to the regulatory framework which can achieve better protection of individuals' privacy while ensuring that personal data can move and be processed freely through the ever-expanding digital economy. BSA believes that the review of the existing framework represents a major

[33] BSA members include Adobe, Altium, Apple, Asseco Poland S.A., Attachmate, Autodesk, Autoform, AVEVA, AVG, Bentley Systems, CA Technologies, Cadence, CNC/Mastercam, Dassault Systèmes SolidWorks Corporation, DBA Lab S.p.A., Intel, Intuit, Mamut, McAfee, Microsoft, Minitab, NedGraphics, O&O Software, PTC, Progress Software, Quark, Quest, Rosetta Stone, SAP, Scalable Software, Siemens, Sybase, Symantec, Synopsys, Tekla, and The MathWorks

opportunity to both improve privacy and boost the digital economy in Europe by crafting forward-looking solutions that are precisely focused to achieve their goals: *maximizing individuals' privacy* and *leaving breathing room* for the *development of innovative and competitive ICT products and services*.

We also believe that a *balanced* and *proportionate* Regulation is needed that can help citizens better understand and control how their data is processed, give regulators a tool that can follow the evolution of the technology it aims to govern, and provide data controllers and processors with the *legal certainty* they need to continue to provide existing services requested by users as well as develop new services. Those characteristics and features, in turn, will foster user trust and confidence in the protection of individuals' privacy, including in the online world. Such trust is essential for the growth particularly of the digital economy.

Workable Solutions to Meet Real Needs

Technology is an integral part of every aspect of today's life and the backbone of every modern economy. People, businesses and governments rely on, and expect, technological solutions to respond to everyday needs. While the explosive growth of the Internet has brought about substantial social and economic benefits, Internet technologies have also fundamentally transformed the landscape of how, where and by whom data is collected, transferred and processed.

The new legal Framework must allow for achievable results and set the right level of expectations. For example, *certain elements of the proposal—particularly those relating to online technologies, such as the Right to be Forgotten, Data Portability, Privacy by Design, Profiling, and the consent regime—need refining in order to make them achievable and consistent with each other.*

The proposed regulation touches upon many of the above mentioned issues/principles with a specific technology, business practice or standard in mind and seeks to address them with very specific rules, regardless of the broader implications and current realities. This runs the risk of raising false expectations for rights which, as currently conceived, may prove extremely difficult to implement and contradict other fundamental rights (eg Right to be Forgotten vs. Data Portability vs. freedom to conduct business).

Ultimately, the strength of the revised Framework will depend on whether it can be implemented in practice, accurately reflects citizens' expectations, introduce much needed legal clarity whilst remaining technology and sector neutral and remains consistent with the architecture and design of key technologies. Overly broad and unreachable goals will provide no solutions at all.

Ensuring a Context and Risk Based Approach to Privacy

The complex nature of today's digital environment has led to an explosion of the use of information technology for everyday communication and information processing. The response of the current proposal to these new developments is to significantly broaden the type of data considered to be "personal data" without consideration for the context in which data is being collected or processed. This is ill-suited to today's complex environment, which requires a more proportionate, flexible and context-based approach to determine what protections should apply when and for which data, considering the different cases of processing and the various levels of potential harm to individuals, to their privacy or to their data.

The current proposal parts from the existing approach by expanding the definition of personal data beyond data that the controller can use to identify the data subject. It defines "data subject" to cover anyone "who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by *"any other natural or legal person"*. This blanket approach does not address the issue of how closely data needs to relate to an individual for identification to be reasonably possible. *There are legitimate reasons and circumstances—such as in the security context—where organisations need to process information potentially relatable to an individual in manners that do not impact anyone's privacy, and which therefore should not trigger the same core obligations and protections as may rightly apply in other contexts*.

The Regulation must recognize circumstances where organizations may have legitimate reasons to process data that otherwise may indeed be personal, as well as cases where, for the controller in question, the processed data does not relate to an identifiable individual, in which case such data should not be classified as personal.

The current blanket approach would make essential online services such as the deployment of security technologies far more challenging, make compliance far more complicated and could lead to the collection of more personal data than needed in order to demonstrate compliance with the Regulation.

- *A context-based approach should be adopted to the definition of "personal data":* data should be personal only if the controller can actually identify the specific person to whom the data relates. Such an approach would be proportionate, as it would recognise that safeguards must apply where data subjects are identifiable by the data controller.
- *The scope of personal data should not be expanded to apply in a blanket manner* to other forms of data, such as location data. The existing definition is flexible enough to cover any data—including location data—where that data relates to an identified or identifiable person.

— *We caution against introducing a "one-size-fits-all" approach to consent* requirements regardless of risk or context. As currently envisaged there would not be any scope to adapt the form of consent to the specific context in cases where anonymous or pseudonymous data is processed; a single requirement for *"explicit"* consent would be disproportionate.

Ensuring an Efficient Internal Market with a Robust Level of Protection for Data Flows in Europe

BSA supports the decision of the European Commission to replace Directive 95/46/EC with a directly applicable Regulation because of its ability to bring legal clarity on the rules that apply and to reduce confusion and inefficiencies associated with the current patchwork of EU data privacy laws. If correctly drafted, a Regulation could bring greater legal certainty for both businesses and consumers and ensure a higher level of privacy for EU citizens. To achieve this, the following aspects of the proposed Regulation are key and should be supported:

— *Main Establishment:* This regime is pivotal to enhancing the internal market. For this to work in practice, complete clarity on jurisdictional competence is needed throughout the Framework. The definition of the main establishment must be based on objective criteria that recognize the nature of today's *global business operations and corporate structures* and allow an organisation, whether acting as a controller or as a processor, to determine its single main establishment and subject itself to the competence of that jurisdiction's supervisory authority. However the current definition may not achieve the desired outcome as different criteria for controllers and processors (many businesses will act as both) will lead to different results and therefore jurisdictions and negate the benefits of the one-stop shop principle.

— *Administrative Burdens:* Drawing from the well-established international concept of "accountability," the Regulation will require controllers and processors to be "responsible" for how they handle data. For example, the Regulation contains many new ex ante requirements, including maintaining records, conducting Privacy Impact Assessments (PIAs) in certain circumstances, and appointing a Data Protection Officer. Controllers also would be required to verify the effectiveness of these measures, which may be carried out by "independent internal or external auditors". These reforms could help keep data safe and build consumer confidence. However we are concerned that, as currently conceived, the Regulation ties the ability to demonstrate accountability to the prior and ongoing completion of a rigid framework of burdensome ex ante administrative requirements. By doing so, it not only increases the regulatory pressure on businesses while denying them any flexibility to choose how best to comply.

— *Administrative Sanctions:* The Regulation introduces high administrative sanctions (up to 2% of the annual global turnover). We believe that a "one-size-fits-all" approach, which applies the same sanctions to deliberate, flagrant violations of the rules as it does to violations that are merely negligent or the case being even accidental, is inappropriate. *The fact that administrative sanctions for non-compliance with ex-ante obligations are based on loosely defined criteria (eg, "negligence"), creates significant legal and financial risk exposure for many companies—particularly smaller enterprises.* High fines, combined with rules that would diminish DPAs' discretion by requiring them to impose fines in every case, could be extremely detrimental to the launch or survival of start-up companies and innovative SMEs, and disproportionate to the potential privacy harm caused to data subjects. Moreover, any automatic infliction of penalties could deter self-reporting, reducing overall transparency, security and privacy. Such a regime would significantly raise the cost and associated risk of introducing new products and services into the market while neither reducing the risks to data being processed nor providing added protection for consumers.

Ensuring Technology Neutrality and Focusing on Substantive Outcomes

BSA members fully support the substantive goals of the Regulation: increased legal certainty, transparency, accountability and clear rules for both providers of data services and users. We are strongly of the view that these goals are best achieved by providing flexibility to entities subject to the Regulation on how best to implement organizational and technological measures and practices to fully comply with the goals of the Regulation while providing breathing room for those entities to adjust and update their implementation as technology continues to improve and evolve and as new threats to privacy emerge. With this in mind, we believe prescriptive rules mandating specific procedures or technologies to achieve privacy outcomes should be avoided because such prescriptive mandates will not stand the test of time, might create single points of failure, and may well dampen R&D and the further development and use of innovative technologies.

Prescriptive rules enacted on the basis of a snapshot-in-time will not lead to an increase in privacy protection standards and practices; highly specific rules will most likely not promote compliance with the rules, but either induce an illusion of compliance without achieving effective protection against real risks, or even outright encourage creative circumvention of underlying policy goals.

— *Secondary legislation:* Throughout the current draft text, for areas such as privacy by design, data portability, security of processing and certification schemes, the Commission is granted substantial authority to adopt delegated and implementing acts. These acts could include introducing technical standards, design requirements and criteria for technical measures and procedures. The Commission's ability to propose secondary legislation in a wide number of areas threatens to complicate, rather than simplify, data protection. If new rules are regularly adopted, it effectively means that the requirements for data protection are always changing and it becomes virtually impossible for enterprises ever to achieve compliance. Further, if the Commission chooses to adopt highly prescriptive measures or dictate specific technology outcomes it could hinder innovation and competition in privacy protection and lead to sector-specific legislation—negating the harmonisation goal of the Regulation.

— *Prescriptive Requirements:* The proposed framework focuses on very specific requirements and mandates how fundamental principles should be applied. In order to deliver effective privacy protection, rules should focus on substantive outcomes rather than on specific procedures. The rules should establish a high level of baseline practices, require companies to be held accountable to them, and be enforceable. Overburdening companies with specific procedures and requirements that do not add protection to citizens will harm competitiveness and innovation, discourage entrepreneurship and new ideas, while also damaging the European market's attractiveness as a place to do business, thereby hindering growth and jobs, increasing costs and prices, and ultimately reducing consumer choice as well as service quality.

— *Profiling:* existing language on "automated decisions" has been extended in the draft Regulation to a loosely-defined category of data processing called "profiling". In doing so the proposal makes two significant and incorrect assumptions: that any automated decision amounts to profiling; and that profiling necessarily identifies an individual. As such these provisions threaten to subject a vast range of legitimate data processing activities—including any processing of anonymous data—to additional controls, without consideration for the actual privacy implications of the processing in question, and without consideration for the many positive applications of profiling and automated processing. BSA recognises that safeguards are needed against data processing that produces negative legal effects or adversely affects a data subject. However profiling techniques and technologies have many positive uses, such as improving or customizing services for consumers, preventing fraud, or various accounting purposes. These have been fundamental to the success of the Internet and of many new business models, and should not be prohibited or unduly constrained moving forward either.

Enabling Online Security

Privacy and security considerations are intertwined, and data privacy objectives can only be achieved if the Internet environment is secure. The framework must therefore ensure security technologies can be developed and deployed based on identified threats, and the privacy goals should be achieved in ways that do not impede the development and deployment of effective security measures.

— The Framework should include an *explicit clarification* in a legally binding article that processing data for network and information security purposes constitutes a legitimate interest. Recital 39 of the current Draft Regulation recognizes this need and should be included in a binding article to ensure legal consistency across the EU and provide legal certainty for companies that need to process certain data to provide network and information security.

— *A harm-/risk-based system for personal data breach notification* is needed in order to prevent over-notification, and avoid desensitizing consumers and overburdening national supervisory authorities. Not all breaches are of equal importance or pose the same level of privacy risk. The notification requirement should be limited to breaches that cause or could potentially cause actual damage ("adverse effects") and should include a safe harbour from notification for data that was unusable, unreadable, or indecipherable through technological protection measures. Further, the currently envisaged 24-hour notification timeline does not give companies sufficient time to properly assess the implications and nature of a breach, or to put in place effective counter-measures, or to even file a notification report that is any relevant or meaningful.

International Data Transfers

European citizens and organisations now routinely move data between countries, both within and beyond the EU, to deliver the services consumers request in the most effective, cost efficient and therefore competitive manner. Flexible and efficient legal mechanisms must be in place to ensure that this can be done, while at the same time guaranteeing the security of data of EU origin regardless of its geographic location. Although we welcome many of the proposed reforms related to data transfers to third countries, we are concerned that under the proposed Regulation, many companies would need to combine different compliance mechanisms with no single solution enabling the data transfers necessary for the activities with a global reach.

— The Regulation introduces important new mechanisms to facilitate the secure flow of personal data, including in the cloud. These mechanisms include new rules on "standard" contractual clauses. We welcome these measures. But we also believe that cloud-based processors and others should be encouraged to go beyond the "baseline" safeguards set out in the Regulation in certain contexts. Where controllers and processors have practical experience that suggests that additional safeguards are appropriate to protect data, they should be incentivized to adopt these safeguards.

August 2012

Written evidence from the Direct Marketing Association of the United States

OPINION ON EU COMMISSION'S PROPOSALS TO REFORM EU DATA PROTECTION LAWS

The Direct Marketing Association of the United States (DMA)[34] is the world's largest trade association dedicated to advancing and protecting responsible data-driven marketing. Founded in 1917, DMA represents thousands of companies and nonprofit organizations that use and support data-driven marketing practices and techniques.

Information is a vital component for DMA members to send relevant offers and requests for donations to the correct audience at the correct time. The use of such data has resulted in tremendous economic and job growth in both the US and UK. According to research conducted by DMA, marketers—commercial and nonprofit—will spend $168.5 billion on direct marketing, which accounts for 52.7% of all ad expenditures in the United States in 2012. Measured against total US sales, these advertising expenditures will generate approximately $2.05 trillion in incremental sales. In 2012, direct marketing accounts for 8.7% of total US gross domestic product and produces1.3 million direct marketing employees in the US. Their collective sales efforts directly support 7.9 million other jobs, accounting for a total of 9.2 million US jobs.

Research published in July 2012 by the Direct Marketing Association (UK) Ltd revealed a projected growth of 7% in the direct marketing industry in 2012 in the UK, from the £14.2 billion spent in 2011 to nearly £15.2 billion forecast for 2012. UK companies profiled in the research attribute, on average, 23% of their total sales to direct marketing, with the travel and leisure and retail and wholesale sectors attributing 30%+ of their sales to direct marketing.[35]

Hiring in the direct marketing sector in the UK is robust as well. It is estimated that industry headcount in 2011 for the direct marketing industry topped 530,000 workers. By the end of 2012, 23% of telecoms and utilities, 15% of business and professional services, and 12% of financial services expect to add direct marketing personnel, while the rest of the UK economy remains mired in recession.[36]

The DMA fully supports the UK Parliament's efforts to forge a path that does not overburden business or other organizations, and that encourages economic growth and innovation. The DMA believes that this is fully achievable while protecting consumers' personal data. In its current form, the General Data Protection Regulation proposed by the European Commission in January 2012 greatly concerns the DMA. The DMA believes that the Proposed Regulation's unprecedented global reach and expansive scope will serve as a trade barrier between the US and the EU, by limiting the free flow of information that powers economic activity between these geographic areas. This, in turn, would not strike the right balance between the need for a proportionate, practicable but effective system of data protection in the EU, and the need for business to be free from stifling regulatory, financial, and administrative burdens.

In response to the Justice Select Committee's Call for Evidence, the DMA wishes to share its thoughts about the UK Government's proposed next steps.

THE DMA SUPPORTS EFFORTS TO INCREASE TRANSPARENCY AND TO PROVIDE INFORMATION TO DATA SUBJECTS AS LONG AS ORGANIZATIONS ARE NOT UNJUSTLY BURDENED BY NEW COMPLIANCE OBLIGATIONS

Article 11 in the Proposed Regulation requires data controllers to have "transparent and easily accessible policies" with regard to the processing of personal data and the exercise of the data subjects' rights. The DMA seeks clarification on whether a privacy policy would comply with this provision, or whether some additional mechanism is required. DMA members already maintain privacy policies and have invested in in providing insight into their data practices through this mechanism. Any requirement for providing transparency through another means would require additional review by DMA members.

The DMA also has many questions regarding the procedures and mechanisms that would need to be put into place in order to let the data subjects' exercise their rights. The DMA questions the one-month deadline for responding to a data subject's request in Article 12, which may put a disproportionate strain on the limited resources of smaller businesses and non-profit organizations. Instead, we propose that the deadline be determined based on a sliding scale taking into account an organization's size.

[34] http://www.the-dma.org.
[35] The Direct Marketing Association (UK) Ltd, "Putting a Price on Direct Marketing 2012" (31 July 2012).
[36] *Id.*

The DMA believes that the language in Directive 95/46/EC (the "1995 Directive") was more nuanced to allow for requests of exceptional size and scope. The 1995 Directive required organizations to provide information regarding data being processed upon a data subject's request "without constraint at reasonable interviews and without excessive delay or expense." In the Proposed Regulation, organizations are now required to provide information within one month of the request, unless the request is "manifestly excessive," an undefined term in the Proposed Regulation.

The DMA Supports An Overhaul Of The Right To Be Forgotten Based Upon Its Impracticality, Cost And Potential For Consumer Confusion Regarding Its Scope

The DMA believes that the proposed "right to be forgotten" reveals a fundamental lack of understanding regarding how companies function and interact with consumers.

The "right to be forgotten" in Article 17 would require companies to erase data about individuals upon request. In practice, EU data subjects already have numerous rights to object to the processing of their data, to have access to their data, and to control the use and processing of data. Another special right, requiring companies to purge all copies of data *and* to inform third parties to purge their copies of data, may not be technically feasible, especially in situations where information has gone "viral." Even in ordinary business situations, the ability for digital media to be reproduced instantly and at no cost to most individuals means that achieving erasure pursuant to the right to be forgotten could potentially only be achieved at great expense. It could also hamper general compliance efforts, or create difficulties with companies involved in internal investigations. The impact of this provision on the common practice of creating backup tapes for servers is also unclear.

Aside from its infeasibility, the DMA also believes that the right to be forgotten strongly undermines fraud prevention and other beneficial purposes for which organizations retain data. It may also contradict other fundamental rights encapsulated by the Proposed Regulation. For example, how can an organization confirm whether it is processing an individual's data pursuant to Article 14 if the data has been erased? How may organizations confirm requests for erasure if they are not permitted to maintain records pertaining to an individual? These are only some of the fundamental points where the Proposed Regulation does not clearly set forth what organizations would be obligated to do.

Other provisions in the draft Regulation would further burden businesses. For example, Article 18 creates the right for data subjects to require a company to provide a copy of all of their personal data in a standard electronic format, to be determined later by the European Commission. Companies rely upon their databases as an integral part of their commercial operations. This provision would allow a business competitor to obtain information contained within another business' databases, simply by incentivizing individuals' to request a copy of that information.

The DMA Supports The UK Parliament's Efforts To Resist New Bureaucratic And Potentially Costly Burdens On Organizations Which Do Not Offer Greater Protection For Individuals

The DMA agrees that many of the new bureaucratic requirements in the Proposed Regulation would impose costly burdens on organizations without providing additional protections to consumers. For example, the Article 33 requirement to include the processing of "personal preferences" data as one of the processing operations that presents specific risks and requires a data protection impact assessment would require almost all marketing activities to be subjected to the burden of producing an impact assessment. This requirement has the potential to bring many marketing activities to a standstill, without any evidence that these activities are harmful to consumers or otherwise impact their privacy. Instead, we suggest that privacy impact assessments be limited to areas where there truly is risk of harm to consumers, such as processing of financial data or health data.

Article 34 similarly creates a large regulatory burden on both organizations and the Data Protection Authorities who will be tasked with reviewing requests from organizations for which the data protection impact assessment indicates a high degree of specific risk. In these cases, although organizations could put appropriate safeguards in place on their own initiative, the requirement to consult with a Data Protection Authority would almost inject a high degree of delay which, in many cases, will operate as an effective denial of the request.

Data Breach Provisions Need Substantial Revision To Promote Realistic Timescales As Well As Sensible And Proportionate Thresholds For Breach Notification

As many others have noted, the 24-hour deadline for breach notification to supervisory authorities imposes an unrealistic timeline. As written, the breach notification provisions in the Proposed Regulation will result in constant breach notifications to local supervisory authorities because every intrusion, no matter how small, will be reported proactively instead of risking the massive penalties in the Proposed Regulation for failure to report. Breach notification would be required for data that was accessed, even if it was not disclosed or used in any way. US organizations have vast experience with the separate breach notification laws in 47 different US states and this experience makes clear that a 24-hour window simply is not enough time to secure the systems involved, enlist the help of law enforcement, and investigate the cause and result of the incident—all common steps to be taken in a run-of-the-mill data security incident. Most organizations will not know basic details, such as what data potentially has been compromised, until the 24-hour window has closed.

Overnotification to consumers will result in "notification fatigue" and endanger consumers who will be too exhausted by overnotification to pay sufficient attention to the notices that truly matter.

Administrative Penalties Should Be Proportionate And Supervisory Authorities Should Be Given Greater Discretion

Much attention has focused on the hefty administrative penalties in the Proposed Regulation. The DMA is concerned that the size of the penalties is excessive in light of the fact that the Proposed Regulation allows for the maximum penalty to be imposed for infractions such as the negligent misuse of a data protection seal or mark or the negligent failure to ensure that the data protection officer has the resources to fulfill his duties. The numerous potential pitfalls for organizations in the Proposed Regulation coupled with the disproportionate penalties will give organizations pause before expanding their investment in the EU.

Providing additional discretion to supervisory authorities will result in a more robust culture of compliance. Even the best intentioned market actors make mistakes, and organizations will want to know that they have the opportunity to work with regulators to correct their errors and ensure the success of future compliance efforts. Under the Proposed Regulation as written, organizations have no incentive to proactively work with regulators when a concern emerges, as an organization will rightly fear that the unjustly punitive nature of the sanctions in the Proposed Regulation will be brought to bear upon it.

Additional Prospective Rulemaking Will Continue To Impose Requirements On Businesses

The Proposed Regulation leaves important issues to be decided by later rulemaking procedures. An important example is found in Article 30, which requires data security measures to be undertaken, consistent with the "state of the art" and the cost of implementation. However, the EC is empowered to adopt delegated acts to determine, among other things, what constitutes the state of the art for various industry sectors. It is unclear whether industry will have any input at all into determinations of what constitutes the state of the art for their own industry sectors. Moreover, the "state of the art" changes rapidly, especially in areas involving digital technology. By allowing a governmental body to make these determinations, these definitions will remain static and suspended in time while industry changes around them.

In other instances, the entire substance of the rule is left to subsequent rulemaking. For example, Article 31 requires notification of a data security breach to the supervisory authority within 24 hours of having become aware of the breach. Yet, Article 31 empowers the European Commission to adopt delegated acts for "specifying the criteria and requirements for establishing the breach" and for the circumstances in which notification to individuals is required. The business community has no ability to assess the reasonableness of these breach notification provisions, since the specifics of when notification is required will not be determined until after the Proposed Regulation is adopted.

There are numerous other examples of this delegated rulemaking. The ability of the European Commission to impose specific requirements and industry standards after the fact does not allow the business community to plan for implementation of the Proposed Regulation.

In addition to the DMA's views on the next steps proposed by the UK Government, it wishes to share some of its other concerns related to how the Proposed Regulation appears to target direct marketing activities disproportionately compared to other industries.

The Proposed Regulation's Focus On Bringing "Behavior" Within Its Scope Would Limit Marketing Activities

The Proposed Regulation would apply to any US company that conducts activities "related to" the "offering of goods or services" or the "monitoring of … behaviour" of EU data subjects. (Article 3) This expanded territorial scope would bring US based companies who offer products and services online via a website accessible within the EU, or who conduct even minimal marketing activities online that include EU residents, within the scope of the obligations imposed by the Proposed Regulation. A more appropriate standard may be to limit the Proposed Regulation to companies that "target" EU data subjects.

The Proposed Regulation targets marketing in other ways. Article 20 gives every data subject the right to refuse any activity that "significantly affects" the person and is based on the automated processing of data including location, personal preferences, and behavior. Most marketing activities are automated, and the automated analysis of data is what allows marketing to work effectively on behalf of consumers.

In another example, the new definition of "biometric data" in the Proposed Regulation includes data related to "physiological or behavioural characteristics of an individual." (Article 4) "Biometric data" is considered to present specific risks to the rights and freedoms of data subjects, necessitating an extensive data protection impact assessment to be produced prior to undertaking any processing activities related to the data. (Article 33) By extension, any marketing activities involving the processing of behavioral information would potentially be subject to the delay and burden of producing this type of assessment.

As the purpose of the Proposed Regulation is to protect individual rights, the Regulation should make clear that anonymized and de-identified data does not fit within the scope of the Proposed Regulation. As currently

written, the Regulation would encompass any information "relating to a data subject" with "data subject" defined as an "identified natural person" who can be directly or indirectly tied to an identifier. (Article 4) Additional clarity in these definitions would help make clear when anonmyzed or de-identified data, which is often relied upon for marketing purposes, and poses no risk to the privacy rights of individuals, are exempt from the Proposed Regulation.

As the Proposed Regulation moves closer to implementation, the DMA's members remain gravely concerned about its effect on economic relations between the US and the EU. In the fragile global economy, the sweeping scope of the Proposed Regulation and the potentially burdensome penalties imposed for even minor infractions will hamper further growth of US companies into EU markets.

The DMA thanks you for allowing us to submit comments in response to the Justice Select Committee's Call for Evidence. We appreciate your consideration.

August 2012

Written evidence from the UK Cards Association and Financial Fraud Action UK

EUROPEAN UNION DATA PROTECTION FRAMEWORK PROPOSALS

1. The UK Cards Association is the leading trade association for the cards industry in the UK. Its members account for the majority of debit and credit cards issued in the UK, issuing in excess of 54 million credit cards and 86 million debit cards and covering the whole of the plastic transactions acquiring market in the UK.

2. Financial Fraud Action UK (FFA UK) is the name under which the financial services industry co-ordinates its activity on fraud prevention, representing a united front against financial fraud and its effects. FFA UK works in partnership with The UK Cards Association on industry initiatives to prevent fraud on credit and debit cards and with other partner bodies on non-card fraud matters.

3. We are grateful of the opportunity to give evidence to the Justice Committee. Our response focuses on those key issues raised by industry in respect of the implications of the proposals on data sharing in both the provision of credit and in the interests of fraud detection and prevention.

Potential Implications Arising from the Consent Requirements

4. Due to the way in which the UK credit industry operates, consent is at the heart of the credit referencing model. In signing the original application, the customer gives their consent to a credit search being undertaken at the credit reference agencies (CRAs) and for data from CRAs to be used in the ongoing risk management of an account. Customers are also notified of the lender's intention to share data through the CRAs once an account is open.

5. If a rigorous interpretation of the EU proposals on explicit consent is adopted, there will be significant adverse, and we believe unintended, consequences for industry. By way of example, if a more onerous requirement were to be applied, lenders may need to obtain new and on-going consent in respect of credit card accounts which have previously been shared (in excess of 50 million records). Looking at the wider credit sector, over 450 million records are currently filed with the credit reference agencies (CRAs). This covers a range of sectors including banks, finance houses, mortgage providers, mail order companies, and mobile phone providers. We do not believe it is practical or proportionate to require explicit consent to be obtained each and every occasion that a transaction requiring reference to data is undertaken.

6. Not only would this be a significant overhead to achieve compliance, but it could also have serious inadvertent consequences such as Claims Management Companies purporting that data should not have been shared in the first place and therefore challenging enforceability of an agreement.

7. As will be appreciated, the payments industry uses data for fraud risk profiling and also in support of intelligence sharing models which facilitate the detection, disruption and prevention of fraud. We believe that there is a sound case for a clearly defined and controlled "carve out" for all fraud prevention activity to allow data usage in this way. There is a danger that if there is any ambiguity over what is permissible the likely outcome for industry, and ultimately the consumer, is a greater risk of and propensity for fraud to occur.

8. Ideally we would seek clarification as to whether Member States may adopt legislation for specified public interests reasons allowing organisations to process data without establishing a lawful basis under Articles 6 & 9.

Application of the "right to be forgotten" and "the right to object"

9. Data that is shared with the CRAs is essential to enable the credit industry to make robust and informed lending decisions and comply with its commitments and regulatory requirements to lend responsibly.

10. The right to be forgotten could have a significant impact on the way that lenders do business if, for example, a customer could choose to have certain data effectively erased. Lenders would have to adopt more cumbersome processes to satisfy themselves that they were lending in a responsible manner as they could not be assured from CRA data alone that they were seeing a complete and accurate picture for any customer.

Additionally, and as a consequence, customers could suffer from "thin files" (less information available reflecting payment histories) which could impact their future ability to obtain credit.

11. Of particular concern is the fact that the Regulation appears to allow data subjects to object without providing grounds for doing so, with the burden of proof now being reversed such that it is the data controller who can refuse any objection if able to demonstrate "compelling legitimate grounds".

12. Adverse interpretation and enforcement of the "right to be forgotten" combined with the "right to object" could mean, in the case of credit data sharing that consumers can have data removed and lenders will be expected to make informed decisions based on incomplete records and with ineffective lending assessment tools available to them.

13. If there is a constraint on the extent of the data that can be held and shared, there would be a very real risk that fraudulent activity would (i) be harder to identify, and (ii) could actually be facilitated and increase. This would be to the detriment of all parties, including UK plc.

14. Given that we believe, and hope that this was supported by the legislation, that there are valid, justifiable and legal reasons for holding financial data, the provision of the "right to be forgotten" could be construed as misleading to the consumer if there are exceptions to the rule. This could lead to frustration and give raise to significant levels of complaint.

15. There is therefore a need for a clear articulation of the purposes and justified scenarios where data can be retained (for the appropriate legislative period).

Privacy by Default

16. The new "privacy by default" requirement mandates that data must not be made available to an indefinite number of individuals. For disclosure of information through fraud detection systems and intelligence sharing models, this requirement would effectively limit the recipient base. If this were to be the interpretation this would significantly limit the effectiveness of such models and we have in previous paragraphs highlighted the impact on fraud detection and the potential to facilitate fraud. We would therefore strongly encourage a clear "carve out" from this requirement to maximise industry's ability to respond to the threat and play its part in the fight against fraud.

Data as part of Collaborative Fraud Data Sharing Initiatives

17. The payments industry is committed to fighting fraud and has invested much time and resource to achieve this objective. This included sponsorship of the Dedicated Cheque and Plastic Crime Unit (DCPCU)—a special police unit fully sponsored by the banking industry.

18. As an industry we are fully supportive of the development of the NFA Intelligence Sharing Roadmap concept, the supply of fraud data to the NFIB, and managing fraud data sharing through FISS.

19. We would not want to see the proposals result in legislation being enacted that will constrain industry and other stakeholders from tacking fraud. In saying this, we are particularly mindful that this is a key focus for Government under Fighting Fraud Together.[37]

Ministry of Justice—Next Steps

20. The majority of the Ministry of Justice's next steps (as detailed in their Summary of Responses document) are very pragmatic and we particularly welcome their comments regarding the need to negotiate for an instrument that does not overburden business, the public sector and other organisations.

21. However, we would raise concern over the reaffirmation of 'the right of individuals to delete their personal data, where this is appropriate' as there needs to be clear articulation of those types of scenario where the requirements of business (or other body) would override that right.

Conclusions

22. We are supportive of ensuring a robust, yet practical and proportionate, data protection model that does not adversely affect stakeholders including consumers.

23. As the proposals are set out, we are concerned that the processes that are currently adopted by industry to maximise its effectiveness in both responsible lending and fraud prevention may be compromised. Ultimately this may reduce industry's ability to operate in an effective and timely manner, impacting not only the businesses concerned but also consumers, the authorities and ultimately UK plc.

24. The UK's data sharing model is more advanced than in many other member states, due to a number of important enhancements which have seen the practice evolve to meet the demands to continue to lend responsibly. As such, the inadvertent consequences from some of the proposals will be more severe for the UK industry and its customers.

[37] http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/fighting-fraud-tog/fighting-fraud-together?view=Binary

25. The requirements if interpreted literally (and unchanged) will result in a high, and disproportionate, cost of compliance for financial institutions. This could ultimately stifle innovations and potentially reduce consumer choice.

26. We would strongly encourage a proportionate approach which recognises the different uses of data and facilitates its use where this is in the interests of all parties.

August 2012

Written evidence from Adobe Systems

EUROPEAN UNION DATA PROTECTION FRAMEWORK PROPOSALS

About Adobe Systems Incorporated

1. Adobe is one of the world's largest software companies, providing solutions that enable our customers to more effectively produce, distribute and monetize digital content. Our software is used by customers in every industry sector and by governments worldwide.

2. As a leading provider of software to both consumers and businesses based in the UK, we fully understand the importance of balanced data protection regulation and are committed to supporting the UK government in securing a positive resolution to the current policy debate over data protection in the EU.

Question One

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

Clarification of applicable law and jurisdiction welcome, but needs further work.

3. Adobe provides services in all 27 EU Member States, and is, potentially, subject to the jurisdiction of 27 Data Protection Authorities. We therefore welcome, in principle, the notion of replacing the Directive with a Regulation provided this change helps clarify the question of applicable law and jurisdiction, and eases the administrative and financial burden of compliance with legislation.

4. Nevertheless, the provisions need to be looked at in greater detail to ensure that a single supervisory authority shall, as far as possible, have jurisdiction over a controller established in their Member State. We would welcome the addition of an explicit requirement on supervisory authorities of all Member States to refer complaints and investigations about a given organisation to the designated supervisory authority. Unless the "lead DPA" model is given real effect, one of the major potential benefits to companies from the new Regulation may not be fully realised.

Broader scope of personal data creates legal uncertainty.

5. We share the assessment of the call for evidence from the Ministry of Justice that a far broader range of information could be brought within the scope of the updated data protection rules. This raises a number of challenging issues:

- The lack of clarity: While recitals 23 and 24 nuance the definition in Article 4 by suggesting that context may be taken into consideration when assessing if data is personal data, this nuance is not given legal weight in the definition itself.
- Article 4 suggests that virtually all "online identifiers" (including cookies and IP addresses) could be considered personal data, subjecting that data (and the controllers and processors that use it) to the full range of obligations outlined in the Regulation.
- The legal status of pseudonymous and anonymised data is unclear. While recital 23 implies that the principles of data protection are not applicable to data where the data subject is no longer identifiable, the impact of Article 10 is not clear. o Given the risks attached to non-compliance (ie sanctions) it is not clear that any company would be in a position to benefit from the flexibility suggested in the recitals, meaning that the broad definition of Article 4 would be likely to apply in practice. The consequences of such a fundamental broadening of scope cannot be easily quantified.

6. The impact of changes in the consent regime requires further analysis. The draft Regulation increases the role of consent as a legal basis for data processing, and adds new restrictions to the conditions for obtaining valid consent. It also limits the conditions under which data controllers can assert their own legitimate interests as the legal basis for data processing.

7. The privacy benefits of an explicit consent model are not clear. Over-reliance on consent is not likely to be a panacea for user privacy as users will have difficulty in assessing the relative importance of different consent requests, resulting in a "click-through" attitude to privacy. Service providers are likely to make authentication and/or acceptance of terms and conditions a requirement for the use of their websites in order

to demonstrate compliance with the Regulation. It is questionable whether a move away from anonymous browsing improves user privacy.

8. Explicit consent changes the relationship between users and the websites they visit, and constitutes a fundamental shift in responsibilities. The economic impact of making such a fundamental change without consideration for the privacy impact of the processing in question, needs greater investigation. Our own statistics show that somewhere between 10–20% of browsers block cookies. Reversing the consent regime to explicit opt-in is likely to affect a range of data processing activities including web analytics, as fewer people accept the data processing for analytics or optimization purposes. As a result, organisations are likely to be faced with operating inefficient websites, creating significant economic waste. This may increase pressure on some sites to charge fees for the use of website services or to access content. However not all sites may want to, or be in a position to, charge for their services at all.

Conditions surrounding withdrawal of consent need clarifying.

9. The "without detriment" test in recital 33 creates the risk that data controllers could be obliged to continue to offer a service to a data subject once consent has been withdrawn. This would potentially oblige an organisation to provide a service without any means of monetising that service, and would unfairly discriminate between users that have not withdrawn consent. This is likely to be true for both paid and free hosted services.

10. The relationship between the proposed draft Regulation and the e-Privacy Directive is unclear. Any investments companies make in compliance with the updated e-Privacy Directive may be invalidated if the provisions on consent in the data protection Regulation are taken to override the e-Privacy Directive. We believe that the UK's pragmatic approach to e-privacy is driving a range of new best practices in terms of ensuring informed consent.

New provisions on "profiling" are likely to impact legitimate data processing activities.

11. Article 33,2,a creates a risk that many banal data processing operations could potentially be captured by the "significant effect" test, which would create greater legal uncertainty with regulation potentially stifling business and public authorities. We welcome the ICO's findings that some forms of data processing are not likely to reach the threshold of "significant effect".

12. Subjecting website optimisation and customisation of content and advertising to the provisions of Article 20 is likely to negatively impact the ability of websites to optimize their online operations. Adobe customers have reported significant benefits from using our web analytics suite. Achieving such efficiency gains is a legitimate part of any online engagement. Overly restrictive data protection regulation which takes insufficient account of the risk and context of individual processing operations could cause significant economic waste and impacting the global competitiveness of the EU economy.

13. If profiling is incorrectly calibrated, it could subject banal data processing operations to the additional restrictions outlined in Articles 33 and 34. This is unlikely to work in practice, placing a huge burden on the DPAs (that need to review each notification) and on the companies (which need to consult the authorities and other stakeholders). Adding this kind of ex-ante control on top of organisations' own efforts towards accountability and the new ex-post sanctions regime is highly restrictive. The precise cost of this will depend on how long deployment of any given solution is delayed. In a fast-moving and competitive e-commerce context such delays are unwarranted and could prove critical.

Excessive recourse to delegated acts creates legal uncertainty.

14. Allowing the EC discretion to create secondary legislation in so many areas, with no specific timescale and unclear scope, creates a framework that will create legal uncertainty over many years to come. This type of uncertainty limits companies' ability to create products and services compliant with the Regulation. It also restricts competition amongst companies in providing pro-user privacy tools since companies would not be aware in advance whether the tool will be compliant with the Regulation. Secondary acts also risk deviating from the principle of technological neutrality and discriminating unfairly between products and services. Mandated technological solutions are generally a very blunt tool, and are likely to unnecessarily intrude upon an organisation's ability to define the best way of complying with their privacy obligations over time. There is a risk that many of the instances of "delegated acts" could create overly prescriptive legislation.

Blurring the definitions of Processor and controller will increase legal uncertainty.

15. Adobe is both processor and controller within the European Union at different times. The existing definitions of processor and controller have provided sufficient clarity to enable us to understand our role in any given situation and to express this in legal contracts with other parties. However we consider that the proposed new text unhelpfully blurs this distinction, notably with respect to documentation requirements in Article 28, cooperation with supervisory authorities in Article 29, and data security in Article 30. The Joint Controller provisions of Article 24 already capture the need to clarify roles and responsibilities. Blurring responsibilities complicates the legal environment for parties who wish to contract with each other, and may inhibit the roll out of new services, particularly in a cloud-based environment.

Conclusion

16. We are predominantly concerned about the impact of a Regulation that subjects additional data elements conventionally seen as non-controversial to more prescriptive control, measured against vague definitions and legal tests, in a one-size-fits-all approach which takes little or no account of the context or scope of a data processing operation and its privacy impact.

17. We believe that a positive outcome to the ongoing discussion is one that balances evolving expectations around data protection with an understanding of the significant growth, and value to consumers, of online services.

Question Two.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

18. Adobe believe that the next steps set out in the summary of responses to the Ministry of Justice call for evidence on the EC data protection proposals are broadly acceptable and we welcome the Government's approach for an "EU level instrument that does not overburden businesses, the public sector or other organisations, and that encourages economic growth and innovation".

19. We believe that the Governments summary of responses takes broadly the right approach in this instance, and that the focus on provision of clear information to end users provides a pragmatic alternative to the rigid proposals around consent. We would welcome further focus on clarification

20. We welcome in particular any efforts at clarifying the text to avoid the imposition of bureaucratic and potentially costly which do not appear to offer greater protection for individuals. While the examples cited by the Ministry of Justice are welcome (mandatory data protection impact assessments, seeking prior authorisation from the supervisory authority for certain processing operations and the mandatory designation of independent data protection officers) we believe that further focus is needed on clarifying the scope of data captured within the new Regulation. As explained in our commentary, the new proposals are likely to create significant legal uncertainty and could bring a wide range of legitimate processing activities under the scope of data protection law.

August 2012

Written evidence from the Association for Financial Markets in Europe

European Union Data Protection Framework Proposals Inquiry

The Association for Financial Markets in Europe[38] (AFME) welcomes the opportunity to respond to the Select Committee's Call for Evidence.

Question 1: *Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practical approach but effective system of data protection within the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?*

Our members welcome the aims of the Regulation to improve legal certainty through harmonisation, to reduce the administrative burden on companies and to provide effective rights to individuals. However, they doubt whether these aims have been achieved in the Regulation as proposed and whether the correct balance between the rights of individuals, the obligations of companies and the wider interest of society has been struck. This is particularly the case where the proposed Regulation makes it more difficult for organisations to protect their customer and employee data from external security threats and to fight against financial crime and where the Regulation risks stifling innovation and growth.

Whilst our members support the intention to remove barriers and create harmonisation of data protection rules at EU level, overly prescriptive or complete harmonisation is not desirable as it cannot take account of different cultures, legal systems and business models, and does not in all cases lead to an increased level of protection for individuals, which is the primary aim of the Regulation. Thus whilst Members welcome many of the proposals, such as the abolition of the general notification requirement, the explicit acknowledgment of Binding Corporate Rules (BCRs) and their expansion to processors, and the concept of the lead regulator, they consider that in some areas the Regulation is overly prescriptive, will be difficult to work with in practice, will be unnecessarily burdensome to business and will provide little or no additional benefit to individuals. Members

[38] AFME (Association for Financial Markets in Europe) promotes fair, orderly and efficient wholesale capital markets and provides leadership in advancing the interests of all market participants. AFME represents a broad array of European and global participants in the wholesale markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other market participants. AFME participates in a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association through the GFMA (Global Financial Markets Association). For more information, please visit the AFME website, www.afme.eu.

will be required to focus on procedural requirements with little value for the data subjects rather than concentrating resources on measures and controls that provide effective protection of personal data.

It is particularly important to ensure there is no unintended frustration of the processing of personal data in the context of preventing and detecting money laundering, terrorism and fraud and other financial crimes which requires the careful monitoring, assessment and investigation of customer data and transactions to protect the operation of the global financial system and markets and to safeguard individuals and their personal data. Members are particularly concerned at the lack of progress at EU level of the harmonisation of legislation addressing, on the one hand, the obligations of financial services firms to prevent and detect financial crime and, on the other hand, firms' obligations to adequately protect customers' personal data.

In general, our Members feel that the Regulation, while re-enacting most of the 1995 Data Protection Directive, includes particular additional elements targeted at specific unregulated industry sectors that may have significant unintended consequences for some other sectors of the economy. The financial services sector is already subject to extensive regulation and oversight, entailing important pre-existing obligations. Accordingly, the Regulation needs, at several points, to ensure that it gives due recognition for regulated financial firms discharging pre-existing legal or regulatory requirements.

It has not been possible to accurately quantify the additional costs of complying with the proposals as they stand, although throughout this response we indicate several of the areas that will generate additional cost. Our Members are most concerned the Commission has stated that the reduction in the administrative burden by having one single law will generate cost savings of €2.3 billion (£1.9 billion), when Members are clear that overall costs of compliance will increase and dwarf any savings seen from harmonisation and the removal of the general obligation to notify personal data processing operations. Members are certain that the cost of complying with new obligations will significantly and exponentially outweigh the costs of those obligations that have been removed. For example, one member estimates they will save £20,000 due to the abolition of the requirement to register with the national data protection authority in each of the countries in which they operate. However, the same member estimates they will have to employ an extra 40 staff to meet the additional proposals in the Regulation. Members also expect to incur significant and prohibitive IT costs to be able to meet many of the proposed new obligations, for example to collect, record and manage the numerous and varied consents granted (and withdrawn) by customers.

We are also concerned about the proposed increase of bureaucratic duties to which the Data Protection Authorities (DPAs) will be subject and the impact that will have on our Members and their clients. Many DPAs already struggle with a lack of resources to deal with BCR applications, model contract approvals and other issues in a timely fashion. The proposed Regulation will further stretch their resources considerably, potentially diverting their focus away from more important issues concerning the protection of individuals and affecting their ability to deal promptly with issues that arise where firms require urgent advice, both to be able to ensure ongoing operations of the organisation and to protect individuals. This may result in the DPAs being seen as a barrier to business if they cannot carry out all of their tasks in a timely manner, and adversely affect the credibility of their role if they are unable to deliver as prescribed.

AFME Members operate across the EU and their principal concerns about a number of proposals in the proposed Regulation which they believe will have a significant and adverse impact on their ability to operate effectively, as well as being detrimental to their ability to provide services to clients, will also fail to achieve the Regulation's main objective of delivering a proportionate and effective system of data protection across the EU. Their principal concerns are set out below:-

> *Main Establishment*—Members feel the definition is unclear and not helpful for multi-national firms as not all decisions about processing activities are necessarily made in one location, making the determination of main establishment difficult if not impossible. Many AFME Members operate on a legal entity basis in numerous Member States via wholly-owned subsidiaries, whilst on an operational basis managing their activities on a business line basis. It is unclear, under the current proposal, whether they will be required to have a separate "main establishment" for each subsidiary or whether their sole "main establishment" may be their global or European headquarters, whichever is located in a Member State. Members believe it makes better sense to have a sole "main establishment" for their corporate group in the EU for their activities across the Union, however they are legally and operationally structured.
>
> As many AFME Members are both controllers and processors of personal data (ie one entity in the Group might be a processor for another entity) it is unhelpful to have a different test for the main establishment for processors (place of central administration) compared to that of controllers.
>
> Members are also of the opinion that a significant opportunity for a true "one stop shop" lead DPA under the new Regulation has been missed which would be beneficial to all data controllers across all sectors. The Regulation gives the lead DPA a co-coordinating role and does not preclude non-lead DPAs from dealing directly with organizations for which a different DPA has the lead role which is not operationally effective or helpful.
>
> *Lawfulness of processing*—In addition to processing personal data for the purpose of providing services to customers, (but on this see our comments on Consent below,) Members also process personal data to comply with anti-money laundering, terrorist financing, fraud and sanctions

legislation, as well as to comply with regulatory rules and guidance and domestic and international codes of good practice. Many AFME Members who operate in the EU are entities controlled by holding companies based in jurisdictions outside the EU, such as the United States and Japan. Such Members also have to comply with relevant legislation and financial regulations of those jurisdictions. Accordingly, Members believe that the opportunity must be taken to provide clarification in the Regulation that controllers *can* process personal data in a manner that enables them to comply with the relevant legal and regulatory obligations and codes of good practice to which they are subject. The risk of not providing such certainty places members in a very difficult position as highlighted in an instance where a national DPA instructed a financial institution to cease monitoring customers accounts even though this was being undertaken to comply with the non EU parent company regulatory obligations, incumbent on the whole company, for anti-money laundering and anti terrorist financing purposes.

Consent—Members question whether the current proposals will really benefit the customer and provide an effective system of data protection. Whilst the Regulation calls for the consent provisions in a contract to be clearly distinguishable from other parts of a contract, when dealing with institutional customers, Members find that data protection is less of an issue for customers than other contractual terms such as termination provisions, intellectual property rights, etc. as the personal data processed is often very limited. Members feel that if the Regulation stands in its present form, this may create issues around the enforceability of other terms in the contract that were not similarly highlighted.

Members also believe that lengthy consent notices will not be read, a concern that DPAs have also expressed in the past. The new lengthy and prescriptive requirements around consent appear to undo all the work to date, including at a regulatory level, to ensure that notices are clear, concise and to the point. There is also huge concern about the implications of having to seek retrospective consents from existing customers to meet the proposed requirements, which will require amending and negotiating complex agreements and/or a huge number of terms, mostly with corporate customers with whom only a limited amount of personal data is processed. The scale of the concern about seeking retrospective consent from existing customers is demonstrated by reference to a 2011 survey by Ernst & Young of 12 Tier I European financial institutions which noted that they have, on average, 26 million customer accounts.

Members are also concerned that, as drafted, the Regulation proposes that consent can be vitiated by any material imbalance in the relative positions of the parties: this may have worrying implications for the relationships between employers and employees, and also, given that consent can withdrawn at any time, with customers where data processed in the context of a fraud investigation may lead to the prosecution of the data subject.

Accountability—Members feel the provisions requiring them to document and to be able to demonstrate so many aspects of compliance will generate an excessive bureaucracy that will bring little tangible benefit to customers and will be harmful to business by increasing costs and making services, particularly in the on-line and mobile world, less accessible and innovative.

Breach Notification—Members feel that the 24 hour notification deadline is disproportionate and counterproductive as in many cases it will be impossible to be clear about the nature, impact and scale of a suspected breach in that timescale. Members advocate taking the approach adopted in the E-Privacy Directive, where firms are obliged to notify their DPA "without undue delay" in order to achieve appropriate flexibility (and consistency in EU law). In addition, as with notifying individuals, firms should only be required to notify the DPA of breaches that pose a risk of significant harm to individuals.

Data transfers—The UK Information Commissioner's Office currently takes a pragmatic view with respect to transfers of personal data outside the EU, allowing firms to self determine adequacy for transfers they undertake. This flexibility will be totally lost under the new proposals. As there is no evidence that any individual has suffered harm as a result of the UK approach, members do not agree that the prescriptive approach suggested is necessary.

Members feel that the requirement that BCRs should be *legally binding* on *every* member of a corporate group is unnecessarily restrictive, and does not reflect the current BCR approach and should be deleted. For example, if the BCR is for Human Resources (HR) data, only those group entities handling HR data need be bound to the BCR. Based on their own experience, Members believe that the Regulation should recognise (as the current rules do) that internal corporate policies can make BCRs effective, just as well as legal commitments. In addition, Article 43(1) appears to require BCR's to be approved by the supervisory authority *and* the European Data Protection Board, which appears to question the authority of the supervisory authority.

Sanctions—Members are concerned that there is no alternative at present to fines as a means of sanction as DPAs do not appear to have any discretion due to the use of the word "shall" rather than "may". It also does not seem proportionate that firms who process very little personal data caught by the Regulations may be fined a percentage of global turnover when a tiny fraction of that global turnover relates to the processing of EU personal data. Moreover, some Members generate between 75–90% of their turnover outside the EU. Accordingly, Members feel that any fines should reflect

only turnover generated within the EU rather than global turnover, and be capped at a monetary limit. Also, for banking firms, it is not clear what is meant by turnover: we are reviewing whether the company law directives clarify the position on this.

Under the current proposals, the current sanctions are disproportionate to the possible harm to individuals that may arise from a breach. For example the maximum fine can be levied for the failure to appoint a Data Protection Officer (DPO), even if there is no evidence of any risk of harm to individuals. Under the current proposals, one member could potentially face a fine of $1,869 million for certain breaches of the Regulation, such as the failure to appoint a DPO, whereas under competition law, the largest fine that has been levied by the Commission for a single breach is approximately €950 million.

The issues highlighted above reflect the *main* concerns of AFME Members. However, they share most, if not all, of the other concerns expressed by those participating in or representing other sectors of the economy.

Question 2: *Will the proposed Directive strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection for police and criminal cooperation in the EU, and on the other for law enforcement authorities to be able to investigate crime without disproportionate financial or administrative burden?*

Whilst Members have primarily focussed on the Regulation, they are concerned that there is insufficient clarity around the interaction of the Regulation and the Directive, particularly in the context of interactions with police and law enforcement authorities in connection with the prevention, detection and investigation of financial crime, anti-terrorism, and enforcement of sanctions.

Question 3: *Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?*

AFME Members support the negotiating stance to be adopted by the UK Government in seeking a measure that does not overburden business, contributes to the Government's growth strategy and, facilitates innovation whilst ensuring that personal data is adequately safeguarded—but they respectfully request the Government to also negotiate to ensure that financial services firms are not prevented by the proposed legislation from complying with their obligations arising under other legislation, regulations and industry codes of practice, particularly in the area of preventing, detecting and investigating all forms of financial crime.

August 2012

Written evidence from the Newspaper Society

EU DATA PROTECTION FRAMEWORK PROPOSALS

1. The Newspaper Society (NS) represents the UK's regional media. Our members publish over 1,100 local and regional newspapers, paid-for and free, daily and weekly, circulating throughout the UK, together with 1,600 companion websites, hundreds of niche and ultra local publications and a range of digital and broadcast services including several local radio stations. Local and regional newspapers are read by 33 million people a week and 42 million users a month visit their websites. The industry employs 30,000 people including 10,000 journalists.

2. The NS believes that the Commission proposals will place unnecessary and unjustifiable additional regulatory and "red tape" burdens on businesses, will create uncertainty both for businesses and consumers, and will stifle innovation and development. We also have specific concerns as to the proposals' possible adverse impact upon freedom of expression.

3. That the proposals are put forward by way of a proposed Regulation is itself a major disadvantage. This deprives the UK Government of any flexibility in implementation or enforcement. The draft Regulation is highly detailed, with provision for additional delegated acts and implementing provisions which could be brought forward without appropriate consultation or scrutiny. In addition to our concerns regarding the current text's impact on freedom of expression, any such unknown future measures could raise similar threats or indeed might even encroach upon issues relating to media content regulation—even though this is not an area supposedly within the Commission's remit.

4. The widened and legally uncertain definitions of personal data, the enhanced requirement for consent, the restrictions upon profiling, the right to be forgotten and the onerous requirements for compliance and notification, all have the potential to adversely affect newspapers' vital advertising and marketing services as well as their sales and subscriptions practices, both print and in respect of online services, and their distribution activities.

5. New online business models, from digital subscriptions via advertising in the digital press to e-commerce, are indispensable for the press. The proposed new EU framework will in our view disproportionately burden

the use and further development of such business models, and will undermine legitimate business processing of data for marketing and advertising purposes.

6. The enhanced requirement for "consent" also has the potential for creating an imbalance between global business models based on log-in systems, for whom it is relatively simple to obtain the required consent of their customers, due to the direct contact inherent in the system with their customers, and those such as most publishers who allow free access to their content without any such restraints. For these businesses a requirement for explicit consent would necessitate a new and possibly unwelcome interposition between the publisher and the "reader"

7. We are concerned that the proposals regarding exemption for journalistic purposes in Article 80 are not sufficiently robustly drafted so as to provide adequate protection for freedom of expression, since it is refers to "the processing of personal data carried out solely for journalistic purposes" . We fear that the inclusion of the word "solely" might provoke a narrow interpretation so as to remove from the ambit of Article 80 processing carried out for a dual purpose. If this were the case, the impact of the "right to be forgotten" in particular, as well as other subject rights, upon newspaper electronic archives and on other publishing activities (eg commercial syndication or licensing of content) would have a potentially huge economic impact—as well, of course, as a equally detrimental impact upon freedom of expression and freedom to impart/receive information. The scope of Article 80 is also inadequate and should be extended to include derogation from Chapter VIII and to *require* Member States to provide for exemptions and derogations for all the specified chapters.

8. The potential detrimental effect upon freedom of expression which could be wrought by the application of a "right to be forgotten" has already been noted by the UK Government. In his May 2011 speech to the British Chamber of Commerce in Brussels, the Secretary of State for Justice, Ken Clarke pointed out that the right to be forgotten "*poses all kind of difficulties*." He said: "*Other voices than mine have raised concerns over its ability to impinge on free speech, and to censor information which has been legitimately circulated in the public domain." "More broadly I worry about the impact on business and the public"....."And then there's the question of how a right to be forgotten could ever work in practice, given that we live in a digital era where information is easily replicated in seconds by customers who voluntarily share data. All told, I'm rather worried that this principle would risk setting up what is an unachievable standard and create public expectations that could only be dashed."*

9. We are also concerned by the proposals regarding international transfers of data. UK based media companies may transfer data to other countries in a variety of ways in the course of their business (as opposed to it being merely accessible from outside)—whether directly related to publishing (transmission of information to and from foreign desks, correspondents or overseas offices), or to production, marketing, personnel or accounting processes which have been out- sourced.

10. We are attaching for ease of reference a copy of the NS response to the Ministry of Justice's Call for Evidence earlier this year. The NS is a member of both the Advertising Association and the CBI ad we therefore also take this opportunity to express our endorsement of their submissions to the Committee, the views of which we entirely share.

August 2012

Written evidence from the Society of Editors

EUROPEAN COMMISSION'S DATA PROTECTION FRAMEWORK PROPOSALS

The Society of Editors has more than 400 members in national, regional and local newspapers, magazines, broadcasting, digital media, media law and journalism education.

It is the single largest organisation for editors and senior editorial executives. Its members are as different as the publications, programmes and websites and other platforms for the delivery of news that they create and the communities they serve. But they share the values that matter:

- The universal right to freedom of expression.
- The importance of the vitality of the news media in a democratic society.
- The promotion of press and broadcasting freedom and the public's right to know.
- The commitment to high editorial standards.

1. Further to various discussions about the commission's inquiries, we agree with the points raised by the Newspaper Society who, we believe, has submitted more detailed concerns to you. We also wholly support the NS' original response to the Call for Evidence in March 2012.

2. The Society of Editors remains unconvinced that the proposals outlined so far would create a practicable and effective system of data protection in the EU and that, in doing so, media organisations look set to be stifled by the regulatory, financial and administrative burdens placed upon them.

3. In relation to some of the Commission's proposals our attention has been drawn to a number of the issues raised in the published Impact Assessment and the overly-burdensome costs and practicality of many proposals. The feasibility of a "right to be forgotten" -measures that would contain a requirement for organisations to report data breaches without undue delay and, where feasible, within 24 hours to both the regulator and to the individuals concerned—is both an impractical and over-ambitious window for even the most good-intentioned organisations to feasibly comply. When taken alongside a scenario that may require data forensic officers and other third party organisations providing intelligence into the nature of the breach to carry out their own assessment, the window appears wholly impossible. Alongside this, as outlined by the Newspaper Society, the enhanced requirement for consent has the potential to adversely affect newspapers' vital advertising and marketing services as well as their sales and subscriptions practices, both print and in respect of online services, and their distribution activities.

4. A "right to be forgotten", in particular, seems to have the potential to be unrealistic and burdensome on data controllers and the requirement that they not only delete their own data, but data held by third parties does not take into account the viral nature of the internet. We also consider it to have the potential for an adverse effect on freedom of expression.

5. We remain concerned that a requirement to conduct data protection impact assessments, as well as a requirement for organisations with more than 250 employees to appoint a mandatory data protection officer, has the potential to be extremely costly and overly-burdensome on businesses. Alongside this, suggestions by the Commissioner that organisations that attempt to charge a user for a data request should be fined up to 0.5% of their global turnover and doubled if a firm refused to hand over data or correct bad information, appears extremely steep for what could be a genuine error. Although the industry has always been clear that it deplores breaches of the Act and has urged the strongest action—including the imposition of unlimited fines—short of custodial sentences to punish them, we are at a loss to see what should have occurred since 2006—and the Ministry of Justice's consultation on knowing or reckless misuse of personal data—to have made further consideration of this issue necessary. Neither the Information Commissioner's Office (ICO) nor the Ministry of Justice has produced any evidence to suggest that there are serial breaches of the Data Protection Act that are going unremedied. Alongside this the Information Commissioner has said publicly that he was satisfied with efforts of the media generally and the newspaper industry particularly to deal with data protection issues.

6. Overall, our concerns with regards to the cost of imposing such measures appear no more boldly than in estimates outlined in the Impact Assessment by certain media organisations that any explicit requirement to minimize the volume of users' personal data that they collect and process, would cost in the region of millions to comply. In effect we have difficulty, overall, in accepting the Commission's claims that the proposals would lead to £2.3 billion costs savings and we fear that the European Commission's proposals, in creating unnecessary regulatory burdens, will complicate rather than simplify data protection controls.

August 2012

Written evidence from the Internet Advertising Bureau UK

EU DATA PROTECTION FRAMEWORK PROPOSALS

1. Introduction

1.1 The Internet Advertising Bureau (IAB) is the UK industry body for digital advertising (online and mobile), representing over 700 businesses engaged in digital marketing, including media owners and ad technology businesses. The IAB's role is to help marketers find the best role for online and mobile advertising, promote understanding and good practice and to ensure a responsible medium. Further information is available at www.iabuk.net.

1.2 The IAB welcomes the opportunity to provide written evidence to the Select Committee. Two out of the three questions that the Select Committee poses are relevant to the IAB and its member businesses. We are happy to provide oral evidence to the Select Committee if required.

2. Key Points

2.1 *The IAB is concerned that the proposals fail to strike the right balance between safeguarding the rights of the citizen and enabling innovative data-driven advertising models, which help fund online content, services and applications making them available to consumers at little or no cost.*

2.2 *We believe the proposals are overly burdensome, restrictive and potentially impracticable for UK advertising business models. We believe the proposals will have a significant impact upon these business models as well as the businesses—many SMEs—that these support, as well as growth and innovation and the UK's status as the world's leading internet economy.*

2.3 *The IAB believes that the proposals will also undermine innovative self-regulatory approaches—such as the EU self-regulatory programme for online behavioural or interest based advertising, explicitly supported by the UK Government—that seek to meet the right balance and are built upon extensive consumer research into attitudes towards the internet, advertising and privacy.*

2.4 *The IAB believes that the scope of personal data has been broadened too widely in the proposals and places a disproportionate burden on businesses providing services that are beneficial to citizens, such as customised advertising and the businesses it supports.*

2.5 *The IAB believes the proposals on the right to object to profiling need urgent clarification as it is clear that other aspects of the proposals refer to discrimination (such as on price) as a result of profiling, as well as the use of sensitive information. The IAB believes the boundaries need to be clearer so that businesses can continue with activities that serve "legitimate interests".*

2.6 *The proposed requirement to obtain explicit consent for processing personal data overlooks a contextual and consumer-friendly approach. The IAB is concerned that consent-fatigue would actually lead to lower standards of consumer protection than more sophisticated forms of transparency.*

2.7 *The IAB supports the UK Government position and next steps, as outlined in the summary of responses to the call for evidence. However, we would urge the UK Government to advocate the expressed concerns on the scope of personal data. The UK Government has yet to provide information on its view on this issue, or indeed whether it will be a priority during negotiations at EU level. As a result would like to see a more transparent process with businesses at UK level so that we can support its negotiating at EU level.*

2.8 *Whilst we acknowledge the importance of maintaining a "fluid" EU negotiating position, the IAB recommends a more formal stakeholder forum at UK level to achieve this.*

3. The Evolving Digital Landscape

3.1 Today's internet is significantly different to that of 1995 and this is to the massive benefit of citizens across the European Union. For example: the RaceOnline 2012 "Manifesto for a Networked Nation" found that offline households are missing out on an average of £560 savings per year and that everyone should seek to inspire people to get online to reap the significant economic benefits.[39]

3.2 Advertising plays a significant role in the development of the internet. It is the lifeblood of the digital economy in the UK, EU and globally. As in traditional media, it is the business model for making (non-publicly funded) content widely available to UK citizens for little or no cost. It pays for much of the content and many of the services online: from search, webmail, social networking websites and price comparison sites, to productivity suites, blogs, video/photo sharing and the majority of news, information and video/entertainment sites.

3.3 According to a recent report for the Boston Consulting Group,[40] the UK is the world's leading "internet economy" with those businesses that engage in online marketing, sales and interactions standing to gain the most. Digital advertising—driven by consumer demand for content and services and faster internet speeds—is

[39] http://raceonline2012.org/manifesto

[40] http://www.bcg.com/media/PressReleaseDetails.aspx?id=tcm:12–100468

the fastest growing marketing medium in the UK outstripping all other advertising sectors. The UK leads Europe in digital advertising and no other country in the world has a higher share of its advertising market (28% of a total £16.99 billion) than online and mobile does in the UK.[41] In 2011, £4.8 billion was spent on online and mobile advertising in the UK, an increase of 16.8% on 2010.[42] The UK ecommerce market—driven by advertising—contributes over £70 billion every year to the UK economy and is set to grow by 13% in 2012.[43]

3.4 Data is the fuel for its continued growth. Data-driven models allow advertising to be tailored to UK citizens. The greater efficiency of these models has reduced the barriers to market entry for businesses of all sizes, allowing the richest mixture of content and services to be made widely available to the public. It also allows advertisers to reach audiences that are more likely to buy their goods or services. We believe EU citizens, businesses and the public sector stand to generate significant benefits from the responsible use of data.

3.5 As with personalised content, tailored advertising (such as online behavioural or interest based advertising) require the internet user to share some information to be useful and, whilst this does not require information that identifies the user, we acknowledge the concerns that might arise and the fact that users may wish to take steps to safeguard their privacy. As a result, the pan-European advertising industry has developed a self-regulatory initiative right across EU and EEA markets with the goal of offering internet users clear, transparent and contextual information about the collection and use of information for this purpose, as well ways this information can be controlled and managed, and ways to turn it off altogether. At the heart of this initiative is a new symbol or icon that is now appearing in advertisements on websites to empower users to have greater information and control. This initiative has the explicit support of the UK Government.[44] More specific information on this initiative can be found at: www.youronlinechoices.eu/goodpractice.html.

3.5 The IAB believes this EU initiative finds the right balance between safeguarding privacy and enabling innovative advertising business models that help to fund content and services that internet users demand and enjoy. This is supported by recent consumer research[45] conducted by IAB UK and digital media company, ValueClick. The research concluded that:

- UK consumers understand the importance of advertising in funding online content and services. 61% of UK consumers believe that the internet would "disappear" without advertising.
- UK consumers want relevant advertising. 55% of UK consumers would rather see online advertising relevant to their interests. Six out of 10 want to see a lower number of relevant ads than a higher volume of less relevant ones and nearly half are happy for relevant advertising to be served to them based upon previous web browsing activity.
- UK consumers also want more information and greater control over online advertising. 62% are concerned about online privacy and the vast majority of people surveyed want some aspect of control or more information about how organisations use consumer information to serve online advertising. 40% of UK consumers want easy access to the information being shared about them and nearly half would like to control the type of advertising they see online.
- Many UK consumers are already taking control. The survey revealed that half of UK consumers had deleted "cookies" in the last six months whilst one in five deletes cookies every week (though not distinguishing between the types of cookie). However, 19% of UK consumers do not take any steps to manage their online privacy.

4. *Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?*

4.1 The IAB acknowledges that the development of the internet (including via mobile and other connected devices)—including the significant increase in the exchange and use of data—means that there is a need to review and update data protection rules across Europe. We welcome the opportunity to streamline these rules to reduce the burdens on businesses operating across markets.

4.2 *However, we are concerned that the proposals fail to strike the right balance, potentially leading to an overly burdensome, restrictive and potentially impracticable set of rules for UK advertising business models. We believe the proposals will have a significant impact upon advertising business models as well as the businesses—many SMEs—that these support, as well as growth and innovation and the UK's status as the world's leading internet economy. We believe it will also undermine innovative self-regulatory approaches such as the one outlined in 3.5.*

4.3 The IAB has outlined these concerns directly (including with supporting case studies) with the Ministry of Justice (MoJ) and the Department for Culture, Media & Sport (DCMS), such as a response to its "call for

[41] www.iabuk.net/about/press/archive/online-advertising-enjoys-highest-share-of-uk-adspend
[42] www.iabuk.net/about/press/archive/online-advertising-enjoys-highest-share-of-uk-adspend
[43] www.imrg.org
[44] See relevant speeches from UK Communications Minister, Ed Vaizey: www.culture.gov.uk/news/ministers_speeches/8992.aspx; www.culture.gov.uk/news/ministers_speeches/8592.aspx; and www.culture.gov.uk/news/ministers_speeches/7997.aspx
[45] www.iabuk.net/about/press/archive/consumers-say-the-internet-would-disappear-without-ads.

evidence" in March this year.[46] In partnership with other supporting organisations (such as the Coalition for the Digital Economy and the Federation of Small Businesses) we published an "open letter" to Ministers Lord McNally, Ed Vaizey and Mark Prisk outlining concerns about the impact of the EC's proposals on growth, innovation and entrepreneurship.[47]

4.4 The IAB has three *primary* concerns with the proposals: the extended scope of personal data (Articles 4, 10 and Recital 24); the requirement for explicit consent for processing personal data Articles 4, 7 and 8 & Recitals 25, 34 and 35); and the ambiguity around the right to object to profiling (Article 19, 20 and Recital 58). We are proposing specific amendments to these proposals, aimed at striking the right balance, and would be happy to share these with the Select Committee.

— *The scope of personal data*
Under existing data protection law, a "data subject" means an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity. In the proposal, data subjects will additionally include those that can be identified by reference to "*an identification number, location data and online identifier*". An "online identifier" is explained further in the Recital 24. It says "*when using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers.*" Some of these new elements can clearly identify data subjects, especially when combined with other data; however in many cases it is not possible to identify an individual through these types of data.

The IAB believes that the scope of personal data has been broadened too widely and places a disproportionate burden on businesses providing services that are beneficial to citizens, such as customised advertising and the businesses it supports. The proposals makes no distinction between the use of data to personally and directly identify an individual (eg a name and full postal address) and the use of data that may be unique to a device but does not directly identify an individual (eg the collection of web behaviour linked to a "cookie", not a real identity). We believe that it would be better to restrict the scope of personal data based on the likelihood of identification of an individual. A broader definition of personal data means businesses will have to ensure that all data collected can link back to an individual, encouraging "data mining"—raising further privacy issues as a result—and proving impracticable, and burdensome requirements for many businesses with complex data sets. This is a point that the Information Commissioner's Office (ICO) has sought clarity on.[48]

Given the expanded definition of a data subject, business will be met with ambiguity as to how they can annonymise data considered to be "online identifiers". At present such non-personally identifiable information can have a high value, assisting business to understand their site analytics for example. It is unclear once rendering such non-personally identifiable information as anonymous whether these datasets will still be considered "online identifiers" from which an individual can be identified in the eyes of the Regulation. Recital 23 of the Draft Regulation states that the "principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable". This is the same wording used in Recital 26 of the Data Protection Directive—but there is no guidance as to how one might not make personal data indirectly identifiable. The ICO has published a report on the anonymisation of data and is currently consulting on the document.[49]

— *Profiling*
The proposals grants the user with the right to object to profile building activities if the profiling can produce legal effects or can *significantly affect* the natural person. Profiling activities are defined as those that evaluate, in particular, a natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. These profiles are often used to provide shopping suggestions, filter search results and direct marketing advertisements to the data subject. Profile building is only permitted where there is a contract with specific safeguards, where it is expressly authorised by applicable law or where the data subject has given his or her consent.

Whilst, at present, the creation of internet user profiles may not be impacted by data protection legislation where the user cannot be identified, the language of Article 20 potentially (and unhelpfully) includes some forms of online behavioural advertising. Under the draft Regulation, the reference to "natural person" rather than "data subject" in Article 20 indicates that this activity is to be regulated whether or not the data would comprise personal data and whether or not data subjects could be identified. *We believe this needs clarification as it is clear that other aspects of the relevant Article within the proposals refer to discrimination (such as on price) as a result of profiling as well as the use of sensitive information. We believe the boundaries should be clearer so that businesses can continue with activities that serve "legitimate interests" and this is a point specifically*

[46] www.iabuk.net/policy/responses/iab-uk-response-to-moj-call-for-evidence-on-ec-data-protection-proposals
[47] www.iabuk.net/about/press/archive/industry-bodies-unite-over-ec-data-protection-proposals
[48] ICO—Initial Analysis of the EC's proposals for a revised Data Protective Legislative Framework: 27 February 2012 http://www.ico.gov.uk/news/current_topics.aspx.
[49] ICO—Consultation on new Annonymisation Code http://www.ico.gov.uk/news/latest_news/2012/ico-consults-on-new-anonymisation-code-of-practice-31052012.aspx

highlighted for clarification by the ICO.[50] The practical consequence of the current drafting is that it is likely that providers are likely to move the point at which users must be registered and "logged in", so that more of the site is only available to users who are logged in. This will result in more data being collected about internet users rather than less.

— *Explicit Consent*
The different types of consent in existing data protection law have been consolidated into one form of consent (Article 7). This also clarifies whether implied consent is permitted. However, this is now at odds with the definition of consent in the revised EU ePrivacy Directive meaning that consent obtained to comply with the UK implementation of Article 5(3) of the revised Directive (transposed into UK law as the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011) will not be sufficient for the purposes of the proposed reforms.

If implemented as drafted, it may then require two consents for some web applications. The proposals provide that the consent may not be "wrapped up" in a general consent to web site terms and conditions, but must be broken out into a separate tick box or privacy statement. As the burden of proof lies with the data controller, it is likely that good practice will develop so that the data controller must record and store the results of this tick or click against the identity of the data subject, possibly through a registration system. To record consent in a way that can identify the user, so as to meet the burden of proof standard, will dramatically increase costs and decrease usability. Studies have shown that the use of registration systems on websites that previously did not require registration have caused a dramatic decrease in users. Third party data processors will be forced to ask the website owner, as data controller, to collect the consent of the data subject on the processor's behalf.

Therefore the requirement to obtain explicit consent for processing personal data overlooks a contextual and consumer-friendly approach. We believe explicit consent is difficult to implement in practice in a digital environment and may place a significant burden on businesses and a cumbersome online experience for users. As well as placing additional burdens on businesses, this approach would also disrupt the online experience for users, who could face constant, intrusive "tick box" consent screens and pop-ups. The IAB is concerned that consent-fatigue would actually lead to lower standards of consumer protection than more sophisticated forms of transparency.

5. *Are the next steps the UK Government proposes to take during the negotiations, set out in the summary of responses to its Call for evidence, the right approach?*

5.1 The UK Government (MoJ) acknowledges the concerns we raised in our response to its call for evidence. The IAB supports the UK Government's position and next steps, as set out in its summary of responses to its call for evidence. In particular that it will *"resist new bureaucratic and potentially costly burdens on organisations which do not appear to offer greater protection for individuals"* (page 34).

5.2 *However, we would urge the UK Government to advocate the expressed concerns on the scope of personal data. The UK Government has yet to provide information on its view on this issue, or indeed whether it will be a priority during negotiations at EU level. As a result would like to see a more transparent process with businesses at UK level so that we can support its negotiating at EU level.*

5.3 Whilst we acknowledge the importance of maintaining a "fluid" EU negotiating position, *the IAB recommends a more formal stakeholder forum at UK level to achieve this.*

August 2012

Written evidence from the Association of Medical Research Charities

EUROPEAN UNION DATA PROTECTION FRAMEWORK PROPOSALS

1. The Association of Medical Research Charities (AMRC) is a membership organisation of the leading medical and health research charities in the UK. AMRC has 125 member charities that together invested over £1 billion into UK research in 2011–12, approximately one third of all public expenditure on medical and health research. Medical research charities are the UK public's favourite cause with over 11 million people donating to the sector on a monthly basis.[51] Our members' research strategies are funded by donations from patients, carers and their families and so are strongly focused on benefiting patients. Many of our members have strong patient groups allied to them and represent the voice of patients and the public who have expressly chosen to support medical research through their donations.

2. The new EU Data Protection Framework will have far-reaching consequences including for medical research. These may impact on the NHS and it's ability to participate in research, something that David

[50] ICO—Initial Analysis of the EC's proposals for a revised Data Protective Legislative Framework: 27 February 2012 http://www.ico.gov.uk/news/current_topics.aspx

[51] Charities Aid Foundation/NCVO report (2011) *UK Giving 2011* http://www.ncvo-vol.org.uk/sites/default/files/clickable_UK_Giving_2011.pdf [accessed 2 August 2012]

Cameron recently highlighted as one of five key strengths that make the UK a great place to invest in the life sciences.[52]

3. I attach a joint statement on the proposed European Union Data Protection Regulation from public funders of medical research, including government-backed organisations and charities, which AMRC as co-signatory supports. The medical research charity sector has three concerns:

- the Regulation should reflect that the public are supportive of their data being used for research and want to have confidence that their data will be protected when they share it with researchers;
- that pseudonymised data be excluded from the Regulation and treated as anonymous data given that such key-coded data is not identifiable at point of use;
- and finally that the government ensure the Regulation is implemented with clarity to avoid ambiguity and unnecessary red tape that could hold back research.

4. We have included a selection of case studies which demonstrate the value of data to UK medical research and attached is a brochure from the recent APPG Medical Research summer reception, which focused on the value of data for medical research. The brochure sets out some of the investment made in infrastructure and resources to collect, store and manage large bodies of data in the UK, which will be affected by changes to regulation. It also includes examples of some of the innovative research projects that successfully use patient data and highlights areas where projects have had difficulty navigating the regulatory frameworks and experienced delay, bureaucracy and poorer project outcomes as a result.

The Public are Supportive of their Data being used for Research

5. The public clearly value research and are broadly supportive of their data being used for medical research. In a recent UK Collaborative Trial of Ovarian Cancer Screening, over 1 million women were contacted by letter and asked to participate; only 32 of those women wrote to complain about being contacted.[53] Further evidence of the public's willingness for their data to be used in research was demonstrated by an Ipsos MORI poll commissioned by AMRC in 2011, which found that 80% of respondents would like their doctor to offer them the opportunity to allow a researcher access to their records, and 72% would like to be offered opportunities to be involved in trials.[54]

6. As noted in the *Summary of Responses,*[55] the new Regulation must allow patients to have confidence that their data will be protected when they share it with researchers. We welcome the derogation for research in the Regulation, recognising that special consideration is needed for the use of data for research purposes, so that confidentiality is balanced with the willingness of patients to make their data available and the legitimate need for access by researchers. It is important to prioritise the protection of Article 83 and ensure that the associated derogations for research are maintained as the Regulation moves through the legislative process.

Pseudonymised Data should be excluded from the Regulation

7. It is not clear whether pseudonymised (key-coded) data comes under the scope of the Regulation. Pseudonymised data ensures that no identifiable information is made available to the researcher but a "key" is held separately by a custodian. Researchers using the data have no access to the key, so cannot use the data to identify an individual patient. However such key-coded databases can allow important data sets to be linked and tracked over time. This form of data is of central importance to many publicly-funded projects, including the four new data centres recently announced with a £19 million investment by government and medical research charities.[56] Researchers at these centres and other institutions use pseudonymised databases to mine the dataset collected by the NHS throughout a patient's life (examples of these databases are provided in the fact box below).

8. If pseudonymised data were to be included in the scope of the Regulation, we believe that this would vastly increase the regulatory burden placed on databases such as these, and increase costs, which would unreasonably restrict vital research, while not significantly improving the protection of identifiable information. We therefore believe that pseudonymised data should not be covered by the Regulation and the scope of the Regulation should be clarified to that end.

FACT BOX: the value of pseudonymised data

The Clinical Practice Research Datalink (CPRD)

The Clinical Practice Research Datalink (CPRD) is the new English NHS observational data and interventional research service, jointly funded by the NHS National Institute for Health Research

[52] David Cameron speech to the Global Health Policy Summit, 1 August 2012 http://www.number10.gov.uk/news/global-health-policy/ [accessed 3 August 2012]

[53] Menon U. *et al.* (2008) *Recruitment to multicentre trials—lessons from UKCTOCS: descriptive study* http://www.ncbi.nlm.nih.gov/pubmed/19008269 [accessed 2 August 2012]

[54] AMRC/Ipsos MORI (2011) *Public support for research in the NHS* http://www.ipsos-mori.com/researchpublications/researcharchive/2811/Public-support-for-research-in-the-NHS.aspx [accessed 2 August 2012]

[55] Ministry of Justice (2012) *Summary of Responses* http://www.parliament.uk/documents/commons-committees/Justice/summary-responses-proposed-data-protection-legislation.pdf [accessed 2 August 2012]

[56] MRC press release (2012) *New centres put health records at the heart of medical research* http://www.mrc.ac.uk/Newspublications/News/MRC008799 [accessed 2 August 2012]

(NIHR) and the Medicines and Healthcare products Regulatory Agency (MHRA). CPRD services are designed to maximise the way NHS clinical data can be linked, to enable many types of observational research and deliver research outputs that are beneficial to improving and safeguarding public health.

INBANK

In 2011, Arthritis Research UK launched INBANK, a research platform and database that will link clinician- and patient-reported data with biological samples and patient outcome data from the NHS. The broad scope and linked data in the database will allow coordinated national research into arthritis and other musculoskeletal conditions. For example, academia and industry will be able to use this to identify eligible and consenting patients for recruitment to clinical studies or examine drug effectiveness and identify side effects post licensing. This requires data to be tracked and linked to individual patients.

The MS Register

The MS Register, launched in 2011, is a focused pilot study that combines an online patient portal with clinical NHS data. Anyone with MS in the UK can enter information about how the condition affects their lives. For patients attending one of the five pilot clinics, their online data can be linked to their treatment data and anonymised, making this combined data available for researchers. The data will improve the delivery of care and could be used to identify potential adverse drug reactions and monitor the safety of new MS treatments.

FACT BOX END

The Regulation should be Proportionate and Consistently Implemented in the UK

9. Disproportionate regulation, implemented inconsistently, results in more delay to vital research. And this in turn slows improvements in healthcare without improving patient safety. We believe that in the absence of clarity on regulatory frameworks, researchers and approving bodies are often over-cautious in their attempt to interpret the legislation. Clarity for users and streamlining the implementation of the Regulation through a simple and clear joined-up approach across relevant authorities is important. For example, SAIL, a national database based at Swansea University linking together a range of datasets (set out in our brochure, page 11), including data on health, environment and education, has been successful at gaining access to national datasets but has been hampered by regulatory hurdles when accessing smaller datasets, such as those held by GP surgeries for whom the administrative burden of individually seeking duplicative regulatory approval is too great.

10. Disproportionate or poorly implemented regulation wastes money and the time of clinicians and researchers, and it prevents patients from achieving their objectives of allowing their data to be used for research. If we can address these issues there is an opportunity for significant improvement in the research sector with consequent benefit to the whole UK life sciences sector—one the government has identified as central to economic growth.[57] We welcome therefore the government's intention to develop a proportionate and effective system that protects people's privacy and supports UK medical and health research.

August 2012

Written evidence from Intellect

EUROPEAN UNION DATA PROTECTION FRAMEWORK PROPOSALS

Purpose

This report provides Intellect's response to the Justice Committee's inquiry into the European Union Data Protection Framework Proposals.

Background

Intellect is the UK trade association for the IT, telecoms, and electronics industries. Its members account for over 80% of these markets and range from blue-chip multinationals to early stage technology companies.

Summary

- Intellect welcomes many of the proposals in the Regulation.
- Intellect would like to see greater sensitivity in the Regulation to the character of the organisation processing data to ensure the burdens on the business and the regulator have a corresponding benefit to individuals.
- Intellect is concerned that the wide definition of "personal data" proposed in the review may introduce unintentional barriers to the processing of data by businesses for the provision of necessary services.

[57] HM Treasury (2011) *The Plan for Growth* http://cdn.hm-treasury.gov.uk/2011budget_growth.pdf [accessed 2 August 2012]

- Intellect recommends the proposed Regulation retain the principle of technology neutrality.
- Intellect would like to see greater clarity on the relationship between the data breach notification regime proposed and the existing ePrivacy directive regime.
- Intellect broadly supports the proposed approach of the UK Government.
  - With regard resisting more bureaucracy with PIAs and DPOs, care should be taken to promote less restrictive wording, rather than their complete removal.
  - Intellect would welcome greater graduation in the proposed penalties structure to take into account the scale and seriousness of the breach, as well as existing measures in place.
  - Intellect would encourage the Committee to ask the Government to consider the domestic legislation that will need to be put in place.

Intellect's Input into the Justice Committee's Inquiry: European Union Data Protection Framework Proposals

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

1. Intellect welcomes many of the proposals in the Regulation which will help businesses. For example, steps towards greater harmonisation of EU laws and, in particular, clarification of the applicable law, based around a country of origin principle (the one DPA or "one stop shop" approach). This will see the removal of the administrative burden of having to notify in all 27 different countries. Still, consistency is needed within the Regulation to ensure that this harmonisation follows throughout the legal framework. Additional positive aspects of the proposals include better defined principles, strengthened individual rights, specific obligations for processors, increased transparency and the encouragement of codes of conduct and seal programmes.

2. However, as the question supposes, some implications of the Framework proposals have been interpreted by industry as overly bureaucratic. There is little acknowledgement that making measures mandatory will be crucial to those organisations which process a high volume of public or customer personal data or sensitive personal data, whilst other organisations will only hold employee data for administrative purposes. The increased burdens on businesses and regulators across the board may not result in a corresponding benefit for individuals.

3. Requirements to keep documentation, carry out PIAs where needed, have someone with responsibility for data protection and so on are all part of good data governance and will ultimately benefit individuals to the extent that they will force organisations to keep data protection on their compliance agenda. However, the Regulation goes further by mandating what documentation organisations need to keep, when they should conduct a PIA, and how a DPO should work and be appointed. This mandation will not necessarily lead to better data protection because the Regulation does not take account of the specifics of the organisation or the risks involved. Therefore, rather than being an effective system the process could be reduced to more form filling and box ticking. In some cases organisations with a high risk exposure will need to go further than the Regulation has prescribed, while in others the measures will not be appropriate. It is critical that the Regulation emphasises that at all times data controllers must adopt measures which are appropriate to the volume and sensitivity of personal data that they process.

4. In addition, balance is not just about burdens, it is also about ensuring that the review introduces a legal framework that ensures individuals' data privacy is protected and secured whilst not introducing barriers, perhaps even unintentional, to organisations processing the data that they need to. For example, the processing of data to enable an organisation to provide online goods and services that citizens actually want or need. The proposed changes to the definition of personal data, which would result in all information having to be considered as personal data, could lead to sectors which need to process data, but may not be in a position to attribute that data to a specific data subject, being compromised. A good example of this is cyber security, particularly given the current online threat environment.

5. The legal framework needs to ensure it can remain relevant, appropriate and up to date as we move forward and the role of data increases. The current Directive has been in place since 1995 and has stood the test of time well partly because of the principle of technology neutrality in the Directive. The new proposed Regulation should retain the technology neutrality that is within the current Directive and so ensure sector specific rules are not introduced. There are concerns that many of the proposals could see the introduction of technology and sector specific rules, particularly where the use of delegated acts is being suggested.

6. In terms of the protection of individuals' data, the introduction of a sector wide data breach notification regime should be welcomed as it has an important role to play. To ensure consistency with the proposal's key tenet of harmonisation this should follow the same direction as the current ePrivacy directive regime. Clarity is needed, so that organisations do not have the burden of complying with two different notification processes and procedures. The data breach notification introduced should be appropriate and not burdensome on either individuals or businesses.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

7. The government's overall approach covers the main concerns raised during the consultation process and represents a strong initial position. The government's push back on the use of delegated acts is welcomed, given the potential for these to lead to the unwelcome introduction of technology and sector specific rules. The UK Government's support for data breach notification should also be welcomed, as is the request to re-examine the "right to be forgotten" proposal.

8. In resisting more bureaucracy with regard to PIAs and DPOs, the Government needs to be careful that it doesn't promote the entire removal of these provisions, but simply encourage less prescriptive wording and allow organisations to assess their risks and respond appropriately. The Government should also take the opportunity to push for a more realistic definition of sensitive personal data, which could be achieved, for example, by amending the wording to allow for processing of sensitive personal data where this manifestly does not impact adversely on the privacy of individuals. This relates to the Committee's first question and the importance of striking the right balance between protecting data and individual privacy whilst also ensuring organisations can process the data they need to in order to provide online services.

9. In terms of the proposed fines/sanctions set out in the Regulation, whilst an effective enforcement regime is an important part of having an effective legal framework, the fines structure as it is currently being proposed lacks graduation in the proposed penalties structure to take into consideration the seriousness of a breach of the Regulation, or the measures and investment that organisations have introduced to demonstrate their accountability in terms of the overall requirements of the Regulation.

10. Intellect would encourage the Committee to ask the Government to consider the domestic legislation that will need to be put into place. The ideal situation would be for one piece of legislation to implement the Regulation, that also contains relevant provisions for both domestic and cross-border processing for the purposes of preventing and detecting crime (and so on), along with the national measures (if any) in relation to articles 80 to 83, which allow member states to set out provisions relating to freedom of expression, health, employment, and history, research and statistics. At the other end of the scale we could imagine seven pieces of separate legislation on data protection that organisations would need to consult—as the Government could choose to implement the above separately.

August 2012

Written evidence from the Direct Marketing Association (UK) Limited

EUROPEAN UNION DATA PROTECTION FRAMEWORK PROPOSALS

SUMMARY

1. Current text of the draft Regulation imposes onerous burdens on organisations which could harm the free exchange of information with consumers, stifle innovation and deter investment.

2. Estimated potential cost of draft Regulation in its current format to UK businesses is £47 billion, with a particularly significant impact on SMEs.

3. We broadly welcome UK Government negotiating position but feel some fine tuning is needed.

1. *Introduction*

1.1 The Direct Marketing Association (UK) Limited (DMA) is Europe's largest trade association in the marketing and communications sector, with approximately 900 corporate members and positioned in the top 5% of UK trade associations by income. The total value of direct marketing to the UK economy was estimated to be £9.1 billion in 2011. This comprises three separate figures; £4.3 billion on expenditure on direct marketing media and activities, £1.1 billion on goods and services brought in by companies to enable the undertaking of direct marketing activity and £3.7 billion on the spending of people employed in the industry as consumers (*Putting a Price on Direct Marketing* The DMA July 2012). The DMA represents both advertisers, who market their products using direct marketing techniques, and specialist suppliers of direct marketing services to those advertisers—for example, advertising agencies, outsourced contact centres etc. The DMA also administers the Mailing Preference Service, the Telephone Preference Service and the Fax Preference Service. The use of personal data in order to deliver targeted marketing is at the heart of our members' activities and core to their business success. On behalf of its membership, the DMA promotes best practice, through its Direct Marketing Code of Practice, in order to maintain and enhance consumers' trust and confidence in the direct marketing industry. The Direct Marketing Commission is an independent body that monitors industry compliance. Please visit our website www.dma.org.uk for further information about us.

1.2 The DMA welcomes the opportunity to respond to this inquiry by the Justice Select Committee on the European Union Data Protection Framework Proposals.

2. *Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them*

2.1 The DMA does not believe that the proposed Regulation strikes the right balance for the reasons as set out below.

2.2 Opt-in/opt-out and obtaining explicit consent

The current proposal demands that organisations would have to obtain explicit consent from consumers by "clear statement or affirmative action" to use their data for marketing purposes unless they were relying on the "balance of interests" justification. While organisations would not necessarily have to get consumers to tick an opt-in box, they would not be able to take for granted that consumers consent to receiving marketing information—even if they have had previous interaction with them and were existing customers of the organisation.

The provision of personal data in return for benefits from commercial organisations is common practice well understood by consumers. More than half of respondents to a DMA survey published in June 2012 *Data Privacy: What the consumer really thinks* were happy to sign up for emails in order to receive special offers. If explicit consent were required for these offers they would become uneconomic for brands, reducing consumer choice.

The practice of driving business growth through prospecting using traditional direct mail channels would become extremely difficult if explicit consent were required for these approaches. This would have a severe impact not only on the Direct Marketing Industry but on the financial viability of the Royal Mail.

We are also concerned that there is continued doubt surrounding the issue of what would constitute "fair processing" when considering the "balance of interests" between the organisation and the consumer. The worst case scenario is that organisations that fail to prove they have properly obtained consent from individuals to contact them with direct marketing messages would have to scrap their contact databases completely. These could be difficult and very costly to replace. There is also the question of what would happen to "legacy data" validly collected under the current legal framework.

2.3 Definition of personal data and consequences for profiling

The new Regulation could class IP addresses as personal data. IP addresses are allocated to an individual device and often such devices might be shared in households, offices and other organisations, such as libraries. Furthermore, individuals connect via multiple devices (pc, laptop, mobile phone, and tablet) and a particular IP address does not specifically reveal individual behaviour but merely the behaviour of a device.

This extension of the definition of personal data would result in web analytics no longer being available to organisations without the express consent of individuals and therefore limit commercial development. In particular brands are using and developing digital direct channels to find new ways of stimulating consumer markets The DMA Report *Putting a Price on Direct Marketing*, July 2012, identifies that the retail sector would be among the sectors hardest hit by the inability to use web analytics for marketing purposes. Even though analysis is concerned with the online activities of anonymised batches of IP addresses, the information itself could be considered personal data and hence off limits to those who did not provide consent. This has very serious ramifications for digital marketers as they would then struggle to chart the journey consumers take from communication to action, or to analyse their behaviour online. Profiling is a legitimate business activity which benefits consumers, giving them more targeted and relevant marketing communications and this proposal would jeopardise that benefit. More than half of respondents to a DMA survey published in June 2012 *Data Privacy: What the consumer really thinks*, actively welcome recommendations based on previous purchases made online.

Classifying IP addresses as personal data would also overlap with the Privacy and Electronic Communications Directive. Doing so would damage user experience of websites: their preferences might not be stored, which would deny visitors a personalised experience with the inconvenience of having to upload their details with every repeat transaction. These two effects would inflict incalculable damage on sales. Respondents to a survey carried out by the DMA in connection with its report *Putting a Price on Direct Marketing*, cited the definition of personal data in the draft Regulation as having the most serious implications for their business.

2.4 The right to be forgotten

The new Regulation proposing to give individuals the right to request organisations to delete any personal information that is held on them has been designed with social media networks in mind. This requirement would certainly stifle innovation for social media platforms, but the consequences of the right to be forgotten reach beyond that.

Organisations that hold an individual's data and pass them to third parties would not only have to delete their information but would also have to ensure that the third party does the same. This is clearly impractical.

For data list brokers, this obviously has enormous and problematic implications and all organisations would also face increased data processing costs.

We welcome clarification from the European Commission that the right to be forgotten would not prevent the use of an individual's data to be held for suppression purposes in direct marketing. However, this needs to be made clear specifically in the text of the Regulation.

The relationship between the draft Regulation and other legal requirements on organisations to keep personal data, for example for audit or anti-money laundering purposes, needs to be made clear specifically in the text of the Regulation.

2.5 Subject access request

Currently, organisations can charge a fee of £10 when supplying individuals with a copy of all of the information held on that individual, to meet a subject access request. Under the new Regulation, organisations would have to supply this information free of charge. The £10 fee does not cover the cost of collating and supplying the information but does, at least, act as a small check to discourage frivolous or vexatious requests. We are concerned that this may lead to an increase in subject access requests being used for other purposes, such as for early discovery at a pre-litigation stage in legal proceedings. (This point was identified in the Ministry of Justice's Call for Evidence on the Data Protection Act 1998 in 2010.)

The administrative burden this places on organisations is huge. In 2009, the Ministry of Justice estimated that UK businesses spend £50 million a year in fulfilling subject access requests through additional manpower costs.

A positive note, however, is that we welcome the proposed provision that a subject access right can be met by providing information to the data subject electronically, if that information is held electronically and the data subject agrees to this.

2.6 Data breach notifications

There are no requirements under the current Data Protection Directive to notify the authorities of serious data breaches but the new Regulation would radically change this. Every organisation that holds personal data would have to notify the ICO and the individuals concerned within 24 hours of any instances of data breaches. Although the current draft is particularly vague on the detail of how this would work, it is difficult to see how the ICO would cope practically with the weight of breach notifications which may, in any case, be of a minor nature. It is not always possible to identify breaches within 24 hours, or to assess the extent or likely detriment of a security lapse. If every data breach has to be reported, regardless of its nature or importance, there is a strong possibility of "notification fatigue" setting in—there is evidence of this effect in the USA where most states have this obligation. There is then a risk that consumers may ignore the notification of a serious breach, where they need to take action in order to prevent identify theft.

2.7 International transfers of personal information to countries outside the EEA

While the rules on transferring personal information to countries outside the EEA may have been made more business-friendly, problems could arise with their application beyond the European Union. The law would apply to any organisation in the world processing information about European citizens, but in a digital world an organisation would not necessarily be aware that they were dealing with a European citizen until they had completed an online registration process. This requirement simply doesn't reflect the reality of 21st century global data transfer practices, and needs to be rethought if it is to be workable.

2.8 Marketing to children

This is an area where a prescriptive "one size fits all" approach may not work. We would prefer to see a risk-based flexible framework here, as recommended in the ICO's *Personal Information Online Code of Practice* [http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online.aspx]

2.9 Cost of compliance obligations

We have concerns about the proposal that organisations would have to keep full records of their data processing activities and supply them to the ICO on request, rather than as a matter of course under current rules. This does raise questions as to how the ICO will be adequately funded to carry out its work effectively.

The additional bureaucratic requirements will certainly create extra administrative costs, particularly for smaller organisations. Implementing the right to be forgotten, explicit consent for data processing and the appointment of a data protection officer will all create additional administrative costs. The requirement for organisations with 250 or more staff to have a designated independent data protection officer takes no account of the nature of the organisation's business and how much, or little, data is handled by them. The cost of these compliance obligations would be most strongly felt by SMEs, which typically employ 250 or fewer people. Of the companies polled for the DMA's report, *Putting a Price on Direct Marketing*, the majority of which were SMEs, 22% stated that the average likely cost to their businesses would be just over £76,000, equivalent to 11% of turnover. This translates to an estimated potential total cost to UK businesses of £47 billion. The

Appendix contains the case studies we submitted as part of our response to the MOJ Call for Evidence on the Proposed EU Data Protection Legislative Framework in January 2012, which give more detailed information about the cost of compliance obligations.

2.10 Sanctions regime

The proposal to levy potential fines of up to 2% of an organisation's global turnover is disproportionate and inappropriate in this context, and could lead to organisations removing their operations offshore, or restructuring into different parts to avoid larger penalties.

3. *Will the proposed Directive strike the right balance between the need , on the one hand for a proportionate, practicable but effective system of data protection for police and criminal cooperation in the EU, and on the other for law enforcement authorities to be able to investigate crime without disproportionate financial or administrative burden?*

3.1 This is outside the scope of the DMA's work.

4. *Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of Responses to the Call for Evidence, the right approach?*

4.1 Transparency of processing

We generally agree with the Government's position. Greater transparency of processing of personal information by organisations should enable consumers to have more trust in such organisations. According to the survey carried out for *Data Privacy: What the Consumer Really Thinks*, 60% of consumers that are really concerned about privacy say that they are happy to provide personal information to companies that they trust. However there is a danger that greater transparency may necessarily entail lengthier data protection statements/ privacy policies. Even if such statements are written in accessible and easy to understand language, consumers may find it difficult to take in all the information because of their sheer length. The Government may want to consider arguing for a layered approach as outlined in the Article 29 Working Party's *Opinion on More Harmonised Information Provisions* WP100 published November 2004. [http://ec.europa.eu/justice/policies/ privacy/docs/wpdocs/2004/wp100_en.pdf]

As stated above, we do not agree with the requirement for organisations to obtain explicit consent for all data processing for all marketing purposes.

4.2 Subject Access Requests

We agree that the Government is taking the right approach.

4.3 Right to be forgotten

We are concerned that consumers may think that they have an absolute right to have their personal information deleted and will therefore be dissatisfied with the legislation when they find that one of the exemptions applies.

4.4 Bureaucratic and unnecessary obligations which do not offer greater protection for individuals

We fully support the Government's negotiating position.

4.5 Data Breach Notifications

We agree with the Government's approach.

4.6 National independent supervisory authorities

We believe that further thought should be given to the way in which national data protection authorities and the European Commission will work together on a common interpretation of the Regulation (the consistency mechanism). Some organisations may not be able to take advantage of the one-stop shop, where one national data protection authority will be the lead authority for that organisation. This will arise where management decisions are taken in each country in which that organisation operates rather at the European headquarters level. The risk of consumers reporting a breach to a national supervisory authority which takes a tougher line ("forum shopping") needs to be addressed.

4.7 Administrative penalties

We agree with the Government's position. It is important that national supervisory authorities do not spend all their time and resources on issuing penalties and are able to provide guidance to organisations on interpreting the Regulation.

4.8 Delegated and Implementing Acts

We fully support the Government's negotiating position.

5. *Conclusion*

The DMA is willing to provide further assistance to the Committee and clarify any of the points made in its evidence. Please contact us if this is required.

August 2012

References

1. DMA report Data Privacy: What the consumer really thinks
http://www.dma.org.uk/sites/default/files/tookit_files/data_privacy_-_what_the_consumer_really_thinks_2012.pdf

2. DMA report Putting a price on direct marketing
http://www.dma.org.uk/sites/default/files/tookit_files/putting_a_price_on_direct_marketing_2012.pdf

APPENDIX

CASE STUDIES SUBMITTED AS PART OF OUR RESPONSE TO THE MOJ CALL FOR EVIDENCE ON THE PROPOSED EU DATA PROTECTION LEGISLATIVE FRAMEWORK

The examples below have been provided by some of our member organisations to illustrate their estimate of the impact on their business of the Regulation in its present draft.

1. Global Marketing Services Provider

The proposed Regulation will add significant additional administrative costs especially around the right to be forgotten, explicit consent for data processing and the appointment and training of a Data Protection Officer. Increased responsibility and accountability of data processors will also place additional administrative costs, plus increased insurance costs against potential fines and penalties.

There is a cost implication in the review and assessments of all legacy systems which collect personal data to make sure of compliance with the new requirements, egPrivacy by Design

It is difficult to quantify the potential additional costs but in staffing and training costs alone, the company would expect this to be in the region of £50,000 to £ 75,000 per year.

2. Data Services Provider to the Retail Sector

New data portability and right to be forgotten clauses could require one off new system development at a cost of £100,000.

Cost of up to £5 million pounds for each year of legacy data (up to a maximum of 7 years) that could not be used if Draft Regulation had retrospective impact on data which had already been collected.

3. Membership Organisation with Charitable Status

General rule requiring explicit consent for marketing would make fundraising via marketing almost impossible.

Increase in call time with regard to information needed to be provided to donor on phone—estimate of additional 10 seconds—means an annual full time requirement of 1.8 agents. Also additional 10 seconds average handling time to back office processes gives an annual requirement of 1.3 full time agents. Total of 3.1 full time agents or additional costs of £90,000 means a requirement of an additional 1800 individual memberships to cover this.

Several of our charity members have said that their ability to fundraise via marketing would be made more difficult. There is also a problem over how much information consumers can take in at a time and at least one charity thought that the extra time it will take to provide the necessary information on privacy could well put donors off the whole process.

4. Financial Services Organisation

Cost of reformulating databases to take account of changes—£ 100 to 500k.

General rule requiring opt-in consent for marketing may lead to inability to market to existing customer database—loss of revenue estimated at around £6 million.

Cost per lead from data list brokers could increase by double.

Cost or responding to a Subject Access Request would be an additional £ 30–50 per request based on system set—up costs and incremental staffing and administrative costs due to changes in procedure in draft Regulation.

Consent requirements would create additional administration, and possible difficulties, for accounts held in joint names.

5. Bureau Cleaning Services (organisation which cleans lists for other direct marketing organisations against preference services files and other suppression files, such as names of recently deceased persons and those who have recently moved house)

General rule requiring opt-in consent for marketing could lead to a 50% drop in data being sent to it for processing.

6. List Broking Company

Changes introduced in draft Regulation could lead to a 50% drop in turnover which would mean closure of business with loss of 26 full time jobs.

7. B2B Telemarketing and Digital Marketing Company

Digital side—adding a consent form to all website downloads—One day's development work at £400 per day.

Adding opt-in telemarketing button to CRM system: One day development work at £560.

Cost of staff training £7,600 per annum.

Cost of updating CRM system with clear statement of affirmative action—require call recording cost £1000's.

8. Global Data Company

Introduction of explicit requirements for consent—loss of revenue in excess of £1 million.

Review, assessment and updating legacy data to comply with new requirements—cost in excess of £500,000.

New data security and breach notification requirements—cost between £100–500,000.

System developments to take account of the right to be forgotten, data portability, removal of fee for subject access requests, privacy by design—one off cost in excess of £500,000.

9. List Broking and List Owning Businesses

Business	*Current turnover £000*	*Current revenue £000*	*Current profit £000*	*Impact of opt-in on turnover £000**	*Impact of opt-in on revenue £000**	*Impact of opt-in on profit £000**
Large broker	3,500	1,000	100	350	100	10
Small broker	1,000	300	30	100	30	3
Total Broking sector	120,000	36,000	3,600	12,000	3,600	360
Large list owner	25,000	20,000	4,000	2,500	2,000	400
Small list owner	2,500	2,000	400	250	200	40
Total List Owners	600,000	480,000	96,000	60,000	48,000	9,600

* Assuming impact of opt-in would lose 80% of names, representing 90% of turnover

In these circumstances, list-broking would no longer be a viable business model and third party list ownership would become a high risk business option.

There are approximately 100 organisations directly involved in the UK in list-broking and list-owning sectors: between 600 and 1000 jobs would be at risk.

Additionally, the cost of customer acquisition would increase for all brands significantly.

Written evidence form eBay Inc

EUROPEAN UNION DATA PROTECTION FRAMEWORK PROPOSALS

About eBay Inc.

Founded in 1995 in San Jose, Calif., eBay Inc. (NASDAQ:EBAY) is about enabling commerce. We do so through eBay, the world's largest online marketplace, which allows users to buy and sell in nearly every country on earth; through PayPal, which enables individuals and businesses to securely, easily and quickly send and receive online payments; and through GSI, which facilitates ecommerce, multichannel retailing and digital marketing for global enterprises. X.commerce brings together the technology assets and developer communities of eBay, PayPal and Magento, an ecommerce platform, to support eBay Inc.'s mission of enabling commerce. We also reach millions through specialised marketplaces such as StubHub, the world's largest ticket marketplace, and eBay classifieds sites, which together have a presence in more than 1,000 cities around the world. For more information about the company and its global portfolio of online brands, visit www.ebayinc.com.

eBay.co.uk currently has over 30 million live listings on the UK site, with fixed price goods accounting for the majority (60%) of items sold globally. Sellers of all sizes, including 160,000 registered businesses and over 100 high-street retailers use eBay as an additional sales channel to reach the UK's largest online shopping audience, across categories including fashion, home & garden, and consumer electronics.

Summary

eBay Inc. thanks the UK Parliament Justice Select Committee for its call for written evidence. We will focus our comments on the proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), in particular:

- In order to achieve a true one-stop-shop and reinforce legal certainty over the determination of the lead Data Protection Authority, proposed definitions of the main establishment need to be clarified further;
- Beyond formalistic requirements, eBay advocates a "context-based" approach to consent;
- Additional exceptions should be included for processing personal data related to criminal convictions which are already enshrined in national data protection laws;
- The right to be forgotten and the right to data portability should be overhauled;
- Bureaucratic requirements should be better balanced with the principle of accountability; and
- Data breach notifications should be proportionate to the actual risk of harm to data subjects.

eBay Inc. Comments on the Regulation Proposal

1. eBay Inc. believes the revision of Directive 95/46 has the potential to ensure a consistently high level of data protection throughout the EU while at the same time facilitating the free flow of information in the Internal Market and beyond. In particular, we believe that the approach chosen by the Commission to introduce a fully harmonised single set of data protection rules applicable throughout the EU, coupled with a one-stop-shop enforcement mechanism, is fundamental to bringing legal certainty and creating a consistent regulatory level playing field across all EU Member States.

2. Overall, the objectives of the proposed Regulation are valid: empowering data subjects by reinforcing control and transparency; reduced administrative burden and simplified processes for data controllers and streamlined enforcement powers for supervisory authorities. However, the spirit of the text tends to multiply precaution mechanisms without adding value to data subjects and data controllers alike (formalistic consent requirements, bureaucratic burdens, systematic data breach notifications). Similarly, some provisions should better match today's reality of data processing in order to be workable in practice (right to be forgotten and right to data portability). Finally, some clarifications are needed to reinforce legal certainty where the European Commission's objectives are to be supported (main establishment and one-stop-shop approach).

3. Given the direct impact of data protection rules on eBay Inc. and the Internet economy in general, we are keen on providing comments that we hope will be considered with attention by the Justice Select Committee in order to make the proposal for a Regulation on data protection a future-proof, growth-driver regulatory framework.

Main Establishment, Applicable Law and Supervisory Authorities

4. While establishing full harmonisation of data protection rules throughout the EU, the Regulation introduces the concept of "main establishment" of a company. The "main establishment" triggers the applicable regulatory jurisdiction within the EU, ie the country whose data protection authority leads enforcement with regard to processing activities.

5. eBay Inc. strongly supports the introduction of a "one-stop-shop" approach with respect to the competence of the data protection authorities. This is particularly crucial for multi-national companies with separate legal entities and different business lines operating in several Member States. It sets the conditions for businesses to

be established in one Member State and service Union-wide, without facing an unnecessary compliance burden of duplicated requirements. However we feel that in order to achieve a true one-stop-shop and reinforce legal certainty for data controllers, data subjects and supervisory authorities over the determination of the "lead DPA", proposed definitions of the main establishment need to be clarified further.

6. The data controller should designate its "main establishment" based on a definition which includes the three following features:

- Article 54 of the Treaty on the Functioning of European Union defining companies should be the relevant starting point for determining the location of an establishment, and this term should then be further narrowed in the Regulation to determine the main establishment for data protection purposes.
- It should be clarified that the designation of establishment for data protection compliance purposes should be without prejudice to such designation for other purposes of EU law (eg, tax, insolvency, other compliance purposes).
- A set of relevant objective criteria should be established, which a group of undertakings can choose from to officially designate its location of "main establishment" as regards Data Protection Law. Here we refer to the European Commission's guidance on Binding Corporate Rules (BCRs), where the "lead" DPA responsible for the evaluation and approval of BCRs is determined on the basis of relevant criteria[58] including the location of the group's European headquarters; the location of the company within the group with delegated data protection responsibilities; the location of the company which is best placed (in terms of management function, administrative burden etc) to deal with the application and to enforce the binding corporate rules in the group.

7. Businesses would have to self-assess their structures and declare their main establishment on the basis of these criteria and such designation should apply to all entities part of the group established in the Union. We believe that this approach would not lead to forum shopping for data protection purposes given all the other factors which are related to the group decision on where to place its headquarters, the fact that rules and enforcement mechanisms will be harmonised by the nature and content of the Regulation, and the important role played by supporting DPAs. On the contrary, we believe that such a single, consistent definition of "main establishment", to be used for all situations, would provide the required level of legal certainty to the benefit of individuals, companies and DPAs alike.

8. Finally, we would support the principle of continuity for companies that have already designated a "main establishment" for data protection matters in the EU. This principle should be part of the factors that define the "main establishment".

Here, we encourage the UK government to take position in favour of a clearer and practical definition of the "main establishment" to allow for a true one-stop-shop that will serve companies operating in the internal market.

Definition and Conditions for Consent

9. While there are six different legal grounds for processing personal data that are equal in importance, consent presents a particular interest as, on the one hand, it allows to connect with data subjects in a direct manner and, on the other hand, it presents significant challenges in terms of the process to obtain it.

10. Policy debates on consent have been structured around the distinction between an opt-in approach (data subjects must provide their consent before data are being processed) and an opt-out approach (data are being processed except if data subjects oppose it). The definition of consent proposed in the Regulation (Article 4.8) tends to reinforce this frame by introducing the requirement for consent to be an *explicit* expression of will, "*either by a statement or by a clear affirmative action*"—corresponding to an opt-in approach. eBay believes this distinction is both obsolete and irrelevant when using today's Internet services. Consent may prove appropriate in certain situations more than others. In this respect, the Regulation should incentivise data controllers to base their processing on consent rather than discouraging them by imposing unnecessary burdens. That is the reason why eBay suggests going beyond a formalistic requirement and advocates for a "context-based" approach to consent.

11. Firstly, we believe that a systematic *explicit* consent is an overly rigid requirement that does not match the realities of online services. Consent can in fact be inferred or implied from the action of requesting a service: for example, when a mobile user gives consent for being geolocated when he requests restaurant recommendations nearby. Yet, even if such action or behaviour is clear, it may not meet the threshold of *explicit* consent insofar as consent which is implied from behaviour is by definition *implicit*.

12. Secondly, the requirement of obtaining an *explicit* consent in a systematic way will prevent data subjects from taking real ownership of their personal data but rather make them mechanically accept any type of processing. The insistence on explicit consent for such a broad range of situations is likely to lead to a "trivialisation" of the experience for data subjects and a devaluation of the action of giving consent itself. If data subjects are asked to take affirmative action too frequently, they are likely to have trouble differentiating between the relative importance of different situations. This means in concrete terms that an explicit consent

[58] European Commission's DG Justice Guidance on how to designate the lead authority in the framework of BCRs, accessible here: http://ec.europa.eu/justice/policies/privacy/binding_rules/designation_authority_en.htm

may well be a valid legal ground in certain situations (for example when sensitive data are at stake) but that in other situations, an implicit informed consent is more adequate (for example for geo-location based recommendations services).

13. Finally, as far as the conditions for consent are concerned, we would like to question the notion of imbalance between a data subject and a data controller (Article 7.4) which would invalidate the use of consent as legal ground for processing personal data. eBay considers that the language proposed by the Commission is too broad and could actually miss its target. Here we envisage situations where a business seller works from home and relies upon eBay for his living. eBay would process data that, although business related, can also be considered personal data as the individual seller would probably use his name and physical address for transactions. This situation should in no circumstances prevent eBay as a data controller to use consent as a legal ground for processing personal data. Similarly, data controllers should not be prevented from using consent when their service is very popular thanks to a network effect. eBay believes the objective of this wording is better addressed on a case-by-case basis through the condition that consent shall only be valid if it is "freely given", in the definition of consent (Article 4.8).

Here again, we suggest the UK government should support a pragmatic approach to consent.

Processing of data related to criminal convictions

14. Article 9.1 prohibits the processing of special categories of data, including data that are related to criminal convictions. For obvious security reasons, eBay Inc. may have to process such data. A key objective when using data is to protect our customers and our operations from fraudulent activities. We do so thanks to sophisticated tools and processes which allow us to identify and counteract illegal activities or practices such as money laundering. We may also use these tools to prevent actual criminals from using our services for further criminal purposes.

15. While we welcome paragraph 2 of Article 9 which lists exceptions to the prohibition of processing personal data that are related to criminal convictions, the Regulation requires a *law* of the Member State or the Union authorizing the processing of criminal data. In order to reinforce legal certainty and harmonisation of practices throughout the EU, we would suggest including the list of exception directly in the Regulation.

The UK Government should suggest including additional exceptions that are already enshrined in national data protection laws, including in the current Data protection Act.

Right to be forgotten

16. eBay understands the rationale that led to the inclusion of a "right to be forgotten" in the Commission proposal. To some extent, this right already exists in Directive 95/46/EC as the obligation to keep data only as long as necessary for the purposes for which these have been collected, coupled with the right in some contexts to have data deleted and the right to withdraw consent, are components of the right to be forgotten.

17. If we do not oppose a right to be forgotten as such, the Regulation should however not create false expectations for European citizens by making theme believe that this right is an absolute. Data controllers may indeed have many perfectly legitimate reasons "not to forget" users' personal data, including for fraud detection, anti-money laundering purposes or other legal retention obligations. In that respect, we welcome the safeguards listed in Article 17.3 and 17.4, which rightfully limit the scope of its application to data that is not required to be retained by controllers for compliance purposes. We would however add to this list the retention of data for potential future dispute resolution.

18. Secondly, we are concerned by the requirement for controllers to "*take all reasonable steps to inform third parties of the request to erase any links to, copies or replications of the data*". First of all, Article 17.2 does not seem to take account of the nature of the Internet. The eBay marketplaces business model, allows sellers' listings to appear, for instance, in third party search results. Similarly, visitors, buyers or any individual can copy, transfer and duplicate the information published on our websites, including personal information. This is part of the principle of openness of the Internet. It maximises traffic and increases the chance that offers will produce actual transactions. We make the information public because our users request it. We do not grant any kind of formal authorisation to third parties to publish that information. Once it is publicly available, we do not have any control on how this data is treated by third parties. It would be therefore impossible for a data controller to comply with this obligation and we suggest the deletion of paragraph 2.

19. Finally, the right to be forgotten should apply to all personal data of a user, meaning that the data subject should not have the possibility to ask for deletion of certain elements and retention of others. Indeed, the structure of our data bases would make it lengthy and costly to offer this level of granularity and involve disproportionate efforts for companies.

We appreciate the UK Government intends to push for an overhaul of the proposed "right to be forgotten" and we hope our comments will help make this right enforceable and convenient.

Right to data portability

20. First of all, we believe that data which has to be retained by the controller for compliance reasons should be excluded from the scope of the portability provision. Article 18 does not foresee any safeguards limiting the right to request transmission of such data to another service. Article 18.2 even explicitly mentions that the personal data must be *withdrawn* from the initial controller. We take the view that Article 18 should include a paragraph limiting the applicability of the right to data portability similar to the list of exceptions mentioned for the right to be forgotten. This includes data that should be retained in accordance with Member States and Union law.

21. Our users' personal data may include data relating to other data subjects (feedback comments on eBay or transaction history on PayPal for instance) which may be protected under the law (banking secrecy) and/or information which may prove to be sensitive. Transmitting this data would potentially present significant risk for the privacy of 3rd party data subjects.

22. Finally, as the example used in Recital 55 suggests, Article 18 is meant to establish data portability rights for user-generated content stored on platform systems to avoid "lock-in". However, it has been drafted to apply to any type of personal data in any type of processing, including non-platform systems (such as Human Resources-systems or Customer Relationship Management-systems). Non-platform systems, such as HR- or CRM-systems, are created serving the purposes of the data controller only. Those systems are filled by the data controller, where platform services are filled by users. This presumably portable information may have a significant commercial value for the data controller. If this was transferable on a standard basis, it would raise highly problematic competition issues as service providers would lose important competitive advantage—which may in turn prove detrimental to the whole economy.

23. Our proposed solution would be to differentiate between user-generated data uploaded by data subjects themselves (such as name, date of birth, email address and so on) and data that is the result of their interaction with the service providers.

eBay calls on the UK Government to raise the issue of data portability during negotiations and the fact that, if not well drafted, it is desirable to remove it from the Regulation and properly assess its impact on other areas than data protection.

Bureaucratic Requirements

24. Accountability can be effectively implemented by taking an ex ante rather than an ex post control approach, thereby reducing the burden on businesses and DPAs, and by granting benefits to companies demonstrating a responsible approach to privacy. eBay has always been a strong advocate of the accountability principle as it encourages controllers and processors to put consumer privacy high up on the agenda, be responsible and accountable with respect to existing privacy risks and put in place policies and processes to mitigate those risks—all beneficial behaviours for data subjects and data controllers alike.

25. However, the spirit of the Regulation tends to duplicate efforts by putting in place both the accountability principle and heavy bureaucratic burdens. Instead of encouraging the use of privacy enhancing measures, thereby reducing the administrative obligations on controllers and processors, it introduces new and onerous requirements that will substantially increase disproportionate administrative burden for businesses without any regard to the potential privacy risks.

26. We encourage EU decision-makers to amend Article 28 by restricting its scope to data processing which poses a significant risk to the fundamental rights of the data subject, especially his right to privacy, thus re-introducing the exemptions of the notification requirement of Article 18.2 of Directive 95/46.

The UK Government have committed to resist new bureaucratic and potentially costly burdens on organisations which do not appear to offer greater protection for individuals. eBay Inc. fully support this approach.

Data breach notifications

27. The proposed Regulation foresees different level of breach notifications depending on the severity of the breach, namely notification to the lead data protection authority (Article 31) and to the data subject whose personal data has been breached (Article 32).

28. As far as notifications to supervisory authorities are concerned, the proposal suggests that they have to be made without undue delay and, where feasible, "*not later than 24 hours after the controller has been made aware of the breach*". However, once a breach is discovered, the organization has to stop it, limit the impact, understand what happened, identify the root cause and figure out who was affected. To achieve all of this in 24 hours is extremely challenging. The priority in such situations should be to resolve the breach, not just to inform relevant authorities about it. We therefore recommend adopting the "reasonable delay" approach, with full accountability of the data controller, rather than imposing a fixed deadline that could, in effect, exacerbate the consequences of the breach. Moreover, we believe data protection authorities should only be notified of data breaches that really matter, ie those breaches *which are likely to adversely affect the privacy of the data subject* and excludes low-risk breaches from the notification obligation. This would have the benefits of (i)

offering incentives to use encryption, (ii) avoid endless queues in DPAs processing breach notifications (iii) make it easier for companies.

29. Regarding notification to users, the objective is to inform them about potential damages and give them time to react and protect themselves. Frequent user notifications will destroy societal expectation of privacy and therefore user notification requirements need to be considered carefully. The aim of data breach notification rules should be to promote best practices in raising data subjects' awareness about a breach, providing them assurance that their personal data is handled in a secure and safe fashion and to propose appropriate solutions. A workable system could therefore be a threshold that is based on the concept of "significant risk of serious harm", which adds granularity to the level of risks that a breach can evolve.

30. Finally, breach notification rules should allow for an exemption where technical protection measures have been implemented to render the data unintelligible. We believe that such a system, as it is currently in effect in eg Germany, leads to a more risk-adequate balance.

We support the UK Government position in this regard.

August 2012

Written evidence from Pearson

EU DATA PROTECTION PROPOSAL

We set out below responses from the Pearson Group to the Justice Select Committee call for written evidence on the new draft EU Data Protection proposals. Pearson will focus its comments on the draft EU Data Protection Regulation.

1. Introduction

1.1 Pearson is the world's leading learning company, with 37,000 people across 65 countries and revenues of £5.9bn. Penguin is the leading English-language publisher in many global markets, and the Financial Times Group helps business people make well-informed decisions. Through names like Edexcel, BTEC, Heinemann and Longman we provide educational materials, technologies, assessments and related services to teachers and learners of all ages. Our goal is simple: to help people progress in their lives through learning.

2. Summary

2.1 Pearson supports and welcomes attempts to harmonise data protection laws across Europe.

2.2 We have serious concerns about the draft Data Protection Regulation in that it does not effectively balance the needs and practicalities of businesses with ensuring a robust data protection system for individuals.

2.3 While we welcome the UK Government's "next steps" for negotiations on this draft, we would urge Government to ensure that the Regulation can be applied practically to businesses, and meet business concerns such as those we lay out below.

2.4 Throughout this document we would refer to our previous submission made to the Ministry of Justice following its initial Call for Evidence on the EU Data Protection proposals. This submission is also enclosed.

3. Responses to Questions

3.1 *Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?*

3.2 The Regulation as proposed does not strike the right balance between creating an efficient data protection system and addressing the practical needs of businesses. The current Regulation's proposals do not ensure a proportionate system of protecting personal data which businesses can effectively administer and manage, meaning that individuals' rights could be compromised as businesses become overburdened.

3.3 We have previously argued in our response to the Ministry of Justice that the draft Regulation fails to address business concerns relating to administrative and sector-specific burdens, the impact on our international businesses and the need for further consideration of digital issues. Our main areas of concern are summarised below:

— *Administrative burden*: The draft Regulation is overly prescriptive, setting out detailed processes, rules and obligations for activity such as data breach notifications with little regard for the administrative and cost burdens to businesses. Conversely, the Regulation has less of a focus on proportionality, meaning that action on data protection must be treated uniformly without regard to the impact of any alleged breach or risk. This administrative burden on businesses extends to various proposals covered in the Regulation, including data breach notifications, the "right to be forgotten", international data transfers and unclear consent requirements and rights of access. Businesses are keen to uphold individuals' privacy rights, and we will take on extra cost and activity to ensure this, particularly where there may be a significant privacy risk to the individual. However, if regulations are not in proportion with the practical reality of protecting data, they will be difficult to enforce and prove unhelpful for customers.

— *Specific business concerns*: Provisions within the Regulation will have a negative impact on specific businesses within Pearson. The Financial Times Group would be affected by potential curbs on freedom of expression suggested in the Regulation, whilst unclear guidelines on data relating to children and personal data could impact on Pearson's educational services.

— *Effect on international businesses*: The Regulation seems far too wide in places, implicating companies outside the EU if they are processing personal data about EU-residing individuals. It would be onerous for international companies within Pearson to try to determine whether their business falls under the scope of the Regulation.

— *Internet-specific concerns*: Aspects in the Regulation do not give sufficient clarity or consideration to burgeoning online services such as the Cloud or social media.

4. *Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of Responses to its Call for Evidence, the right approach?*

4.1 The Government's next steps go some way to addressing businesses' concerns and ensuring a healthy balance between business needs and the rights of individuals. However, specific areas of the Regulation which are not addressed in the next steps remain of concern to us. We urge Government to go further to secure a Regulation capable of delivering an effective and proportionate system of data protection. Those concerns not addressed in Government's next steps are outlined below.

4.2 Consent requirements: As expressed in our previous submission to the Ministry of Justice, we seek clarification on a number of requirements proposed around consent, including the level of proof of consent (Article 7 (1)) and definitions which cause uncertainty for our businesses, particularly our education services managing data relating to children (Article 8). We would also need confirmation that the draft Regulation does not propose that consent must be opt-in. Any changes to the existing consent regime would be confusing for customers and they would have significant costs and cause undue burdens to our businesses, which again could have a negative effect for customers.

4.3 Additionally, there would be far-reaching implications if the consent regime is made stricter. It could result in an even greater divergence to countries outside EU, and in particular the US, thereby adding to confusion for individuals, increasing the burden on businesses who target users outside EU and potentially putting UK-based companies at a disadvantage to overseas entities.

4.4 Personal data definitions: The definition for personal data is too vague, causing uncertainty for our businesses. Specific problems relate to whether IP addresses would be defined as personal data (Articles 4(2), 10 and Recital 24), and narrowing the definition of "biometric data" (Article 4 (11)). Our assessment and testing services would also be unduly affected by the proposed definition of personal data.

4.5 Freedom of expression exemption: We would seek clarification that the data protection laws do not unnecessarily impinge on the right to freedom of expression for journalistic purposes, and we seek specific re-wording of Article 80 (1) to strengthen this requirement. The rights of data protection must be balanced with this equally important human right.

4.6 Scope of the Regulation: The draft Regulation could apply to companies outside of the EU if they are processing data of individuals in the EU. The scope is far too wide and it would be difficult and impractical for companies to enforce.

4.7 Internet-specific concerns: Government's next steps do not specifically address issues arising from the Internet, or acknowledge the lack of future-proofing within the current wording of the Regulation. We have previously raised concerns around whether Online Behavioural Advertising would be caught under the Regulation's profiling provisions (Article 20), forcing restrictions on our businesses and investments. Our education services also profile students who use our products, meaning that this important activity could be caught by the profiling proposals.

4.8 We are also concerned as to how the Regulation would affect our work and progress in the Cloud given the scope of the Regulation applying to companies outside the EU processing data (Article 14 (1g)), and the extra costs that would most likely be imposed should the data portability provisions be taken forward (Article 18). We also have questions on how protection by design/default would work (Article 23). How is this process

measured, and how will it impact on products and services that are often changed in a very gradual and piecemeal fashion?

5. Responses to Government's Proposed Next Steps

5.1 [The UK Government will] support the provisions requiring transparency of processing, including the new transparency principle and the requirements for data controllers to provide accessible and easy-to-understand information about processing.

5.2 [The UK Government will] support the requirement for additional information to be provided to data subjects both proactively and in response to subject access requests (subject to consideration of the additional costs), but resist the proposal that subject access rights be exercisable free of charge.

5.3 We welcome Government's support of provisions to enhance transparency in data processing and rights of access. It is crucial that information concerning data is communicated to individuals in an open, clear and transparent manner.

5.4 While we support these transparency provisions, we welcome Government's opposition to free subject access requests. This speaks to a wider point made in our previous submission, requesting that Government recognise the extra burden and costs that will be placed on businesses in managing unnecessary and inappropriate requests. The use of subject access requests for purposes that are not legitimate (for example, as a route to disclosure) is an increasing problem for business—and an area of some confusion with ICO guidance differing from case law. This Regulation gives an opportunity to clarify the law and ensure that this right is used legitimately. Given that managing subject access requests takes time and incurs extra costs, it is important that those requests we take forward are legitimate and appropriate. We urge Government to clarify and reinforce these principles through the Regulation.

5.5 Examples where the Regulation proves disproportionate include the Provision Requirements in Article 14, which are not restricted by the level of sensitivity of the data involved, meaning that standardised, lengthy disclosures will be published and will often go unread by individuals. Not only will these be unnecessary in the majority, but they also come at an extra cost to businesses to produce. Subject access requests will also have a direct impact on our specific businesses, particularly our testing and assessment services. We welcome Government's recommendation that information provided to individuals should be subject to consideration of additional costs, and we seek clarification on where these additional costs would supersede subject access rights.

5.6 [The UK Government will] push for an overhaul of the proposed "right to be forgotten" given the practicalities and costs and the potential for confusion about its scope for both organisations and individuals; however, the Government reaffirms its commitment to the right for individuals to delete their personal data, where this is appropriate.

5.7 We welcome the acknowledgement from Government that the proposed "right to be forgotten" presents a raft of impractical measures and extra costs for businesses, without offering any further certainty to individuals. We agree that an overhaul of this proposal is necessary.

5.8 This proposal will be extremely difficult to implement in practical reality, and there is a strong likelihood that it contradicts other laws and regulations. We would seek clarification on how and when data can truly be deleted. We are also keen to ensure that individuals would not have free reign to delete their personal data when our businesses still have legitimate use and need of it—and for the individual's own benefit. Finally, as stated in our previous submission, we would want to emphasise that the proposal and any subsequent changes to it do not impact on freedom of expression for journalistic purposes.

5.9 [The UK Government will] resist new bureaucratic and potentially costly burdens on organisations which do not appear to offer greater protection for individuals; examples of this include mandatory data protection impact assessments, seeking prior authorisation from the supervisory authority for certain processing operations and the mandatory designation of independent data protection officers.

5.10 We agree with Government's recognition of the financial and practical burdens that will be placed on businesses and organisations through the practical application of this Regulation. Whilst we will use every measure and process necessary to ensure our customers' data is protected, the Regulation's requirements must be proportionate to what we can realistically and practically enforce. We raised specific concerns about the extra time spent on requirements for prior authorisation from the supervisory authority for some types of processing, particularly around international data transfers (Articles 34, 41 and 42). The Regulation should be placing more emphasis on the security of the data stored in the online systems and who has access, rather than focusing on when a data transfer occurs.

5.11 There are a range of other areas where these concerns could apply. Documentation of processing activity, for instance, could incur unnecessary costs, without offering any further protection to individuals (Articles 28 and 29). Nevertheless, where these measures provide real security and benefits for our customers, we will always aim to implement them.

5.12 The UK Government will] support the introduction of data breach notifications both to supervisory authorities and affected individuals, but only if the provisions reflect the timescales needed to properly

investigate a breach and if a sensible and proportionate threshold is provided which excludes minor and trivial breaches from the scope of the requirement.

5.13 We welcome Government's support for modifying the provisions around data breach notifications. We agree that the provisions should be more practical by incorporating a materiality threshold and have more consideration for timing constraints. As we have said in our previous submission, 24 hours is an unworkable time-line to notify supervisory authorities of data breaches.

5.14 [The UK Government will] reaffirm its commitment to a strong and independent supervisory authority at national level and support the establishment of a consistency mechanism to ensure a degree of harmonisation in the application of data protection rules across the EU, whilst allowing independent national authorities some flexibility in how they use their powers.

5.15 We welcome Government's consideration for national authorities to retain some control so as to maintain stability when implementing the Regulation. We support attempts by the Commission and UK Government to harmonise regulation around data protection, which will strengthen businesses across the EU and ensure more certainty and stability as data transfers increase across member states.

5.16 [The UK Government will] support a system of administrative penalties for serious breaches of the Regulation's requirements, but push for a more proportionate level of maximum fines, which allows supervisory authorities greater discretion in applying the powers available to them.

5.17 We support Government's recognition that fines must be administered at proportionate levels. This speaks to the wider point that proportionality will be key if the Regulation is to be workable in practice.

5.18 [The UK Government will] push for the removal of many of the powers for the European Commission to make delegated and implementing acts, particularly where these have the potential to make a big difference to fundamental requirements and principles (for example, the legitimate interests upon which data controllers can rely to make their processing lawful or the safeguards that must be established to allow profiling to take place).

5.19 We welcome Government's acknowledgement of the level of delegated and implementing acts, which could cause uncertainty and impracticalities as businesses attempt to implement the final Regulation.

5.20 The negotiations in the Council of the EU and in the European Parliament are ongoing and are likely to last until 2014. During this time, as new proposals and amendments are put forward, the UK Government may seek additional evidence from stakeholders and interested parties. Assuming that texts can be agreed by the European Parliament, the Council and the Commission, Member States, including the UK, will need to consider how best to implement the legislation (although the Regulation will be directly applicable, some provisions are likely to need to be addressed by domestic legislation).

5.21 We will be happy to supply Government with additional evidence and views throughout the process of these negotiations, and during the implementation of the legislation.

August 2012

Written evidence from Aimia

EU DATA PROTECTION FRAMEWORK

1. Summary

1.1. Aimia is a global leader in the management of loyalty schemes and is entrusted with the personal data of over 280 million customers through over 100 loyalty programmes in 20 countries.

1.2. We are pleased to set out in this submission Aimia's response to the Justice Select Committee's call for evidence on the EU Data Protection Framework proposals, prompted by the European Scrutiny Committee.

1.3. Key points include:

- An ambitious regulatory framework is required to increase accountability and transparency, while avoiding inconsistencies and unnecessary burdens for consumers and businesses.
- We are therefore supportive of EU-wide reform and we welcome the direction of the UK Government's policy.
- Companies should adopt a principles-based approach to data to complement legislative and regulatory requirements.
- An EU Regulation will ensure better consistency and coherence, providing greater legal certainties for consumers and businesses.
- Consent should not always be explicit provided it is informed; transparency, as outlined in article 11 of the Regulation, is key.
- Clearer and simple rules will help businesses to address lack of consumer trust.

— While we support the extension of data breach notification, we believe that the 24 hour target for notification currently stated in the proposal is extremely difficult for data controllers to respect.

2. Introduction

2.1. Our business model requires consumers to trust the way personal data is collected and processed, as they will only be willing to sign up to our programmes if they have confidence that their personal data is safe.

2.2. The declining cost of data storage and the ever-higher processing power has made it possible for companies to collect and analyse increasingly large amounts of data from consumers all over the world, across several country jurisdictions. Therefore, we are supportive of EU-wide reform which achieves an ambitious regulatory framework capable of increasing accountability and transparency, while avoiding inconsistencies and unnecessary burdens for consumers and businesses.

2.3. We welcome the direction of the UK Government's policy as set out in the summary of responses to its call for evidence, and below we set out Aimia's perspective on a number of the issues raised.

3. Consistency of Privacy Rules

3.1. Aimia welcomes the Commission's choice of proposing this reform as a regulation. This legal tool will ensure better consistency and coherence in the transposition of Data Protection rules across Europe, thus improving legal certainty for consumers and businesses. This will remove inconsistencies and complexities of different national regimes. Such an EU-wide approach will simplify business planning and also lower the barriers for entry for businesses that want to grow internationally.

4. Consent

4.1. We welcome the strengthening of provisions relating to consent. However policymakers must be careful not to create legislation that proves burdensome for consumers to manage.

4.2. Aimia does not believe that consent should always be "explicit" provided it is informed. Recurrent pop-ups including lengthy legalistic explanations are seldom valuable information for consumers, and mostly result in a lengthy tick-the-box exercise. Transparency, as outlined in article 11 of the Regulation is the most important attribute. Well implemented transparency and informed consent should be sufficient to give users full control, while ensuring consumer experience is not hampered by repeated interruptions.

4.3. Like the UK Government, we are wary of legislating for a "right to be forgotten" which could lead to dramatic and expensive changes to businesses' technology and also be impossible to police, considering the vastness of the internet.

5. Transparency

5.1. Ensuring transparency from businesses is an effective way of ensuring consumer empowerment, without stifling business. We particularly support the requirement for clarity, accessibility and plain language in policies relating to personal data. We believe clearer and simple rules will help businesses to address lack of consumer trust in several areas including loyalty schemes, where currently 21% of consumers interviewed across seven countries said that they have refrained from joining a loyalty programme due to security concerns (Source: http://datasecurity.edelman.com). These changes will support the consumer and business.

6. Privacy by Design

6.1. Aimia supports the EU proposal's objective of raising the average level of data protection. We believe that privacy by design is the right policy tool to achieve this goal, by encouraging organisations to consider data protection at all stages of collection and processing.

6.2. The last EU-wide overhaul of data legislation was 1995. Given the fast moving pace of technological change and business innovation in response to changing consumer requirements, it is imperative that companies also adopt a principles-based approach to data to complement legislative and regulatory requirements which may be left behind by evolving practices.

6.3. Privacy by design is already a reality in Aimia, which is underpinned by a set of principles that all employees dealing with data have to thoroughly apply at all stages of interaction with our customers' data. We call it TACT: an acronym that stands for Transparency, Added Value, Control and Trust. For information on how TACT please see: http://www.aimia.com/Theme/Aimia/files/doc_downloads/WhitepaperUKDataValuesFINAL.pdf

7. Notification of Personal Data Breaches

7.1. Aimia supports the extension of data breach notification obligations to all data controllers as this helps improving protection standards and promotes trust amongst consumers. However, we think that the EU proposal should foresee proportionate risk-based breach notification rules in order to avoid any unnecessary burden on national data protection authorities. On a related point, we believe that the 24 hour target for notification

currently stated in the proposal is extremely difficult for data controllers to respect. We agree with the UK Data Protection Authority (ICO), that an obligation to notify breaches "without undue delay" would be equally effective, as far as consumer protection is concerned.

8. Data Protection Officers

8.1. We agree with the principle of instituting the position of Data Protection Officer, in order to function as a point of contact with Data Protection Authorities and consumers for all data-related issues.

8.2. However we believe it would be preferable to link this requirement to the quantity or type of data processed by a given organisation, rather than linking this obligation to the number of employees in a company. Moreover, we believe the independence of the Data Protection Officer position requires further consideration, in order to establish a link between the new position and the governance of a company.

9. Data Portability

9.1. Aimia recognises the merits of data portability, in the interests of providing consumers with a greater ability to transfer their data from one platform to another. Aimia is involved in the midata project launched by BIS, although this differs to the data portability position proposed by the draft EU regulation as it is focused on enabling data to be downloadable in a machine readable format to enable consumers to make comparisons of charges made by different service providers.

9.2. We believe that data portability obligations must be carefully evaluated and tested to establish clear parameters for the level and volume of data which is subject to portability, and also to ensure that the process of transmission does not interfere with ongoing business processes.

10. About Aimia

10.1. Aimia Inc. ("Aimia") is a global leader in loyalty management. Aimia's unique capabilities include proven expertise in delivering proprietary loyalty services, launching and managing coalition loyalty programs, creating value through loyalty analytics and driving innovation in the emerging digital and mobile spaces. Aimia owns and operates Aeroplan, Canada's premier coalition loyalty program and Nectar, the United Kingdom's largest coalition loyalty program. In addition, Aimia has majority equity positions in Air Miles Middle East and Nectar Italia as well as a minority position in Club Premier, Mexico's leading coalition loyalty program and Cardlytics, a US-based private company operating in merchant-funded transaction-driven marketing for electronic banking.

10.2. Aimia is a Canadian public company listed on the Toronto Stock Exchange (TSX: AIM) and has over 3,400 employees in more than 20 countries around the world. For more information about Aimia, please visit www.aimia.com and follow us on Twitter: https://twitter.com/AimiaInc

August 2012

Written evidence from the British Medical Association

HOUSE OF COMMONS JUSTICE SELECT COMMITTEE INQUIRY INTO THE EUROPEAN COMMISSION'S PROPOSALS FOR A REGULATION ON THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (GENERAL DATA PROTECTION REGULATION) COM(2012) 11

The British Medical Association (BMA) is an independent trade union and voluntary professional association which represents doctors and medical students from all branches of medicine all over the UK. With a membership of over 149,000 worldwide, we promote the medical and allied sciences, seek to maintain the honour and interests of the medical profession and promote the achievement of high quality healthcare.

This submission is in response to the following question put forward by the Justice Select Committee:

> "Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?"

Executive Summary

— The BMA welcomes attempts to increase protection of personal data and recognises the need to update Directive 95/46/EC in light of advances in technology.

— The BMA welcomes the strengthening of provisions related to consent.

— The BMA is extremely concerned that provisions relating to data for historical, statistical and scientific research purposes remove current patient confidentiality safeguards.

— The BMA is concerned this regulation will have significant additional administrative and processing implications for data controllers and data processors gathering and holding health data.

Fundamental Principles

1. The BMA recognises the need to update data protection legislation but feels the proposals lack clarity regarding the rights of the data subject and the obligations on data processors and data controllers, particularly where this is in a healthcare or clinical research setting.

Consent

2. The BMA welcomes the strengthening of provisions related to consent. The BMA suggests that the definition of consent provided under Article 4.8 should also include the requirement that the person has the capacity to understand what they are consenting to.

Processing for Historical, Statistical and Scientific Research Purposes

3. The BMA recognises the invaluable contribution of high-quality ethically approved research to underpin quality, patient safety and innovation in healthcare. However, the BMA is concerned that provisions relating to data for historical, statistical and scientific research purposes remove current patient confidentiality safeguards.

4. The draft regulation allows personal data to be processed for historical, statistical or scientific research purposes when anonymised or pseudonymised data cannot be used. The draft regulation does state that data enabling the identification of a data subject must be kept separately, but clarification is needed to determine if this can be on a separate database or if it must be stored outside the organisation.

5. The BMA has serious concerns that Article 83 appears to permit the processing of health data, in identifiable form, for research purposes without any reference to consent. The only safeguards which appear in the clause seem to be that identifiable data must be kept separate and researchers can use identifiable data only if research cannot be fulfilled by using non-identifiable data. This seems to significantly lower the existing standard for protection of health data. In the UK there are robust requirements in place for maintaining confidentiality and consent for identifiable data. The BMA would be opposed to any change to the current requirement that any disclosure of confidential information requires consent by the patient (or lawful proxy) unless subject to current exceptions. These existing systems are in place to ensure that patient information can be used for research purposes when identifiable information is required and it is not possible to seek consent[59]. Our understanding is that article 83 as written will permit researchers to use identifiable data without consent or recourse to the section 251 process.

Administrative and Processing Implications

6. The BMA is concerned this regulation will have significant additional administrative and processing implications for those holding and gathering health data. The draft regulation proposes that data controllers will have one month to respond to subject access requests (SARs). This is a reduction from the current timescale of 40 days. The BMA is concerned that this will create additional administrative challenges when combined with a possible rise in the volume of SARs received by healthcare providers.

Data Controller and Data Processor

7. The draft regulation sets out the obligations and responsibilities of the data controller and the data processor. While this has brought clarity to the duties of the data controller and data processor, it also brings additional requirements in relation to maintaining documentation and carrying out assessments. The BMA welcomes this clarification but stresses the need for these duties to be proportionate to ensuring a high level of data protection.

8. The draft regulation also states that where data is processed jointly, data controllers need to determine respective responsibilities for compliance. The BMA is concerned with these provisions, as this has been an ongoing area of discussion in the UK in relation to shared electronic records and is yet to be fully resolved.

Erasure—a Right to be Forgotten

9. The draft proposals provide for personal data to be deleted by the individual concerned and the abstention from further dissemination of that data, provided there are no legitimate grounds for retaining it. Our understanding is that this is particularly relevant to social networking sites—however, clarification will need to be sought with regard to whether this will apply to health records, which cannot currently be deleted in the UK because of the importance of maintaining an audit trail.

Right to Data Portability

10. The data subject will have the right, where personal data are processed by electronic means, to obtain a copy of this data in a portable electronic and structured format, which allows further use by the data subject. The BMA seeks clarification as to how this will apply to health records, which, in their current form, may not

[59] Approval under section 251 of the NHS Act 2006 is the mechanism by which the common law duty of confidentiality can be set aside in certain circumstances.

be structured adequately for further transmission. The BMA is also concerned this could potentially lead to fines for GP practices, Clinical Commissioning Groups and other healthcare providers.

11. The BMA believes there is a need to clarify the provisions of Article 79.5 (d) as it relates to fines for failure to provide data in an electronic format, but does not specify if this only relates to instances where the personal data are processed by electronic means. This clarification is needed to ensure it corresponds to Article 18.

August 2012

Written evidence from CBI

EUROPEAN DATA PROTECTION FRAMEWORK PROPOSALS

1. The CBI is the UK's leading organisation, speaking for some 240,000 businesses that together employ around a third of the private sector workforce. With offices across the UK as well as representation in Brussels, Washington, Beijing and Delhi the CBI communicates the British business voice around the world.

2. The CBI welcomes the opportunity to provide evidence to the Justice Select Committee for this important inquiry on the European Data Protection Framework Proposals. Our evidence focuses solely on the proposed regulations for general and commercial data protection.

3. Business welcomes the objective of harmonising data protection rules across Europe, to simplify the landscape for both businesses and consumers. However, the CBI believes that the Commission's proposals will struggle to achieve this objective and actually risks creating further confusion for consumers. The high costs of compliance and legal ambiguity could risk stifling innovation and deterring investment at a time when we need it most. This submission argues that:

- Poorly defined rights will create headaches for consumers, employees, regulators and businesses.
- High costs of compliance and legal ambiguity will stifle innovation and deter investment.
- Government must continue to press for a much more balanced approach to data protection.

Poorly Defined Rights will Create Headaches for Consumers, Employees, Regulators and Businesses

4. In proposing a European Data Protection Regulation the Commission aims to give consumers greater clarity and control over how their personal data is used, and to strengthen the European single market.[60] However, as they stand, the Commission's proposals risk creating greater headaches for consumers, employees, regulators and businesses alike.

New consumer rights will create confusion

5. Newly-envisaged individual rights include a "right to be forgotten" and a "right to data portability". These new rights are designed to help consumers but will have the opposite effect, and many businesses feel that the rights are, in practice, unworkable:

- A "right to be forgotten" (RTBF) is misleading for consumers as many forms of customer data held by, for example, banks, insurers, employers and public authorities are required to be held for specific periods by law. These would not be subject to the "right to be forgotten" and requests from consumers to have data removed would be frustrated, leading to complaints and litigation. The principle that data should only be kept as long as necessary, which is included in the current Directive and the proposed Regulation, serves the same purpose without creating unrealistic expectations.
- The RTBF is also difficult to apply in an open online environment where the ownership of published data is not always clear. For example the administrators of many online platforms cannot realistically exercise full control of how posted data may be used or reproduced by third parties, and thus requirements to notify third parties if a user withdraws their personal data are technically unfeasible.
- We believe that a "right to data portability" (RTDP) will create confusion for consumers, whilst deterring investment in innovative products and services. Subject access requests already guarantee very similar access rights for consumers and could create enormous costs for businesses having to modify their IT systems to ensure portability, so we suggest that the RTDP should be removed from the Data Protection Regulation to eliminate confusion and uncertainty with existing data protection rights.
- In addition, the RTDP does not seem an appropriate fit for the regulation since it aims to address specific online challenges, whereas the regulation as a whole is intended to be a horizontal instrument, covering all sectors in whatever way personal data are being processed; and because it broadens the scope of the regulation beyond the protection of personal data to facilitating how consumers use their data between different organisations for more competition-related objectives.

[60] EC COM(2012)9/3.

Unrealistic breach notification requirements will swamp authorities and consumers with poor quality information

6. The proposed requirement that data controllers notify Data Protection Authorities (DPAs) of all data breaches within 24 hours, and data subjects "without undue delay", may result in an unhelpful number of notifications for both Authorities and consumers, and may negatively impact the quality of analysis that data controllers can carry out before making notifications. Similar data breach requirements, when proposed in the US, led to concern about "notification fatigue" amongst consumers. Of all the businesses the CBI has spoken to about these proposals all believe it would lead to an increase in costs rather than any savings.

7. In the case of a serious data breach in a large organisation identifying, analysing and quantifying the full scale of a data breach often takes time. Requiring notification within 24 hours may lead to poor quality information being provided to DPAs. The requirement in the E-Privacy Directive "without undue delay" is much more pragmatic. Many businesses feel that a more risk-based approach on data breach notifications is needed, so that the requirement to notify is only applicable where the threat of significant harm to data subjects is identified, or perhaps via the use of a "traffic light"-style framework for grading data breaches.

Creating a "tick-box" approach to data protection will help neither consumers nor businesses

8. The Commission's proposals contain several rules which appear to add to businesses costs without delivering clear benefits for the consumer, simply adding layers of bureaucracy and paperwork to activities where neither consumers nor businesses would wish to see them.

9. The planned broad requirement for any data controller collecting or authorising the processing of personal data to carry out a data privacy impact assessments (DPIA), and the further stipulation that data controllers "seek the views of data subjects or their representatives on the intended processing" in the course of the DPIA, are prescriptive and will have the effect of turning an internal good practice activity into a formal, externally monitored requirement that will have further specified rules and regulations attached to it at a later stage.[61]

10. There is also a risk that consumers will encounter many more unwanted boxes to tick and consent requests to complete when carrying out everyday activities. Under the proposals, if businesses do not gain explicit consent from a customer for each data processing operation they carry out, they may have to prove that the processing was in either the customer's "vital interests" or the firm's "legitimate interests".[62] Given the scope for legal ambiguity in this framework firms may simply judge it safer to gain customers' explicit consent every time a processing operation is carried out.

11. Consumers' everyday experiences could be heavily affected by the above, as carrying out activities such as using price comparison sites or purchasing durable goods may require the user to agree to various forms of data processing and sharing along the way. It is unlikely that a consumer concerned with finding the cheapest flight, or registering a warranty for a newly purchased stereo, will wish to go into detailed explanations of each and every way their data may be processed. In doing so, consumers may lose sight of the choices most significant to them, leading many to simply "tick" the boxes they are presented with, which defeats the intended purpose of being transparent to the customer. The new requirements risk reversing progress made in keeping consent and notification wording concise and understandable for the consumer.

High Costs of Compliance and Legal Ambiguity will Stifle Innovation and Deter Investment

12. The Commission's case for a new Data Protection Regulation partly rests on the benefits the Commission claims it will deliver to European businesses in terms of costs savings and greater legal certainty. However the Commission's proposals as they stand will have the opposite effect and, when considered in full, the costs of compliance and the new risks involved in data processing will outweigh the benefits from harmonisation and deter innovation and investment.

The financial benefits of harmonisation have been over-estimated and the costs overlooked

13. The Commission estimates that European businesses will benefit to the tune of €2.3 billion (£1.9 billion) from the proposed changes.[63] These changes are believed to accrue from reduced administrative burdens as a result of greater Europe-wide harmonisation. However, many businesses question how these figures have been reached and raise concerns that added costs of compliance and financial risks will wipe out any potential savings and likely result in much higher overall burdens. Moreover, for those enterprises that do not transfer data across borders there appears to be little contained within the proposals which will not cut into their bottom line.

14. For many businesses new costs as a result of the proposed changes would include the revision and issuance of new terms and conditions to customers, amending IT systems, revising employee guidance and procedures, training staff and increased documentation of all data processing. One major international finance provider estimates that the total cost of drafting, administering and sending a letter to existing retail customers about policy changes amounts to around £15 per customer, amounting to a six figure sum. In addition, the

[61] See: Article 33(4).
[62] See: Article 6(1).
[63] EC SEC(2012)73, p 8.

company would need to equip their call centres to deal with queries and handle issues arising, the additional cost for which could be in the region of £100,000.

15. The requirement for all organisations with more than 250 employees to appoint a Data Protection Officer (DPO) who must then be employed for two full years is similarly costly and disproportionate, especially for organisations where data processing forms only a tangential part of their overall activities. Recent job advertisements typically show that a qualified DPO in the South-East of England could earn anything between £30,000 and £75,000 per annum. Data protection lawyers can command in excess of £200,000 per annum, and these salaries will inevitably rise if DPOs become a mandatory requirement. Many businesses will need to drastically increase their data protection resources to comply with the new administrative requirements (eg documentation of all processing, DPIAs, breach notifications), which could be particularly difficult for small businesses. The envisaged changes in the Data Protection Regulation could also vastly expand the role of the ICO, requiring considerable extra resources.

16. The Commission's proposals about collective redress are also concerning. Although support to data subjects regarding data protection is useful, it should be supportive only. Bodies, organizations or associations taking over and bundling supposed infringements could lead to business models based upon buying and exploiting claims. This risks creating a claim culture, where organizations stop innovating or have to take huge insurance policies, at the expense of the consumer cost or products and services.

17. The relationship between the proposed regulation and the Directive on Privacy and Electronic Communications 2002/58/EC, which already contains rules for how personal data should be handled in a digital context, is very important for a number of businesses who will be subject to obligations under both. Industry needs further clarity to establish how Article 89 in the Commission's proposals should be applied and how the regulation and directive are intended to operate in practice.

A lack of clarity in definitions will lead to greater uncertainty and legal risk

18. Ambiguities within various key definitions in the proposed Regulation will leave firms uncertain about the precise legal risks of collecting and processing different types of information. The definition of personal data is a case in point. The Commission's current approach to classifying data is to make a binary distinction between that which is "personally identifiable" versus that which is "non-personally identifiable". But this distinction over-simplifies the nature of data as it operates in the real world. A broad definition of "personal data" means that any information which could be used, either directly or indirectly, to identify a living individual will fall under the control of the Regulation.[64] This will cause headaches for service providers as the status of indirect identifiers (Eg Internet Protocol addresses) remains unclear.[65] This lack of clarity in the definition of personal data feeds into uncertainty around other key principles such as consent and user profiling. The definition of "main establishment" and "group of undertakings" also needs further clarity.

19. One of the aims of the Commission in reviewing and re-drafting Europe's data protection framework is to create greater legal clarity and certainty for European consumers, regulators and businesses, but unless the Commission reconsiders its definitions uncertainty and legal risk will increase.

Restrictive controls may preclude innovative services and business models

20. Innovation is the main driver of economic growth, and many innovative business models are based on deriving revenue streams from using data in new ways. There is already a huge challenge for many industries to adapt their business model to new digital platforms while ensuring a solid revenue stream. Data sharing is one way of addressing this, in which businesses can yield huge benefits for both businesses and customers, allowing customers to achieve greater functionality and businesses to expand their revenue base. The music streaming service, Spotify, allows users to share data about their favourite tracks and playlists with friends with a single click. Since June 2011 Spotify users have also been able to sign into Facebook and integrate their Spotify data with their Facebook profile. Since integrating its user data with Facebook's in June 2011, Spotify has added over 7 million more users, and customers are now able to listen to and share music in a legal, more social way. This is just one example of social media, which now plays a huge role in the way consumers share information about news, leisure activities and online shopping and helps support an internet advertising industry worth £4.8 billion in 2011. Yet proposed rules around the treatment of personal data, such as the right to be forgotten will make it much harder for such services to be rolled out to consumers.

21. Supporting free-to-use online content through selling advertising space is at the heart of many of the most popular websites and online news providers. But maintaining a revenue stream from online advertising relies on using better quality data to maximise visitor "click-through" rates. The viability of online advertising is severely threatened by the Commission proposals such as the requirement of explicit consent for processing a wide range of "personal" data, with knock-on effects for many content providers reliant on advertising revenues. The Commission must consider the unintended effects of restrictive data protection rules, before European consumers lose out.

[64] Article 4.
[65] See: Recital 23 and 24.

22. But it is not only online operators that will be affected; restrictive and burdensome provisions will threaten innovation across the board. Organisations in many sectors will want to offer more personalised and globally available goods and services, and are increasingly required to do so to stay competitive. The new data protection framework therefore needs to ensure that the data protection rights of individuals and the benefits for customers, business and society as a whole are appropriately balanced.

Increased processing costs will deter investment and consumers may lose out

23. Data-intensive industries are a major source of growth. The Digital Agenda for Europe aims to make the EU a global leader and investment hub for the digital age. However, many of the Commission's proposals will add significant extra costs and administrative burden to processing Europeans citizens' data. These extra costs will factor into European firms' investment decisions, especially for industries where data collection and processing forms a central part of their business model.

24. Moreover, the Commission's proposals on extra-territoriality (subjecting non-EU firms who collect or process EU citizens' data to the same rules and punitive measures as EU firms) will create a disincentive for non-EU firms to serve EU customers. Ultimately it may be the European consumer who loses out as businesses may simply choose not to provide their services to EU citizens, or indeed simply ignore the rules altogether. It is not difficult to envisage a situation in which a web-based service physically located in the US asks users during the sign-up process whether or not they are an EU citizen. If the individual answers "yes" then access might be reduced or even denied, whereas if they answer "no" they would essentially exempt themselves from EU data protection safeguards. It is doubtful that this would feel like an improvement from the European consumer's perspective. Therefore, we are concerned that the extra territorial impacts of proposed rules should not impact on the ability of industry to export data, and should limit negative impacts on inwards investments to the UK, and more broadly to Europe.

Punitive fines represent disproportionate approach

25. Many businesses are concerned that the proposed 2% fines are disproportionately high and that the DPAs have no discretion in their application. It also does not seem proportionate to use global turn-over as a measure for a regulation companies that generate the majority of turn-over outside the EU of for companies. A more proportionate alternative could be to impose a monetary limit and cap the scope to EU, rather than global, turn-over.

Government must Continue to Press for a much more Balanced Approach to Data Protection

26. Given the significant concerns that the business community has over the Commission's proposals on data protection, it is vital that the Government continues to push for a much more balanced and proportionate approach to regulation in this area. The Government's current approach, set out in the Summary of responses to its Call for evidence strikes an appropriate tone of supporting many of the Commission's objectives while pushing for a more proportionate, practical and technology neutral way of achieving those outcomes, which we support.

27. The CBI particularly supports the Government's position on the following issues:

- Resisting the proposal to waive the charge for subject access requests, since the current nominal charge helps deter unnecessary inquiries.
- Pushing for an overhaul of the right to be forgotten, which as we have noted could cause a great deal of confusion for consumers.
- Resisting new burdens on business such as data protection impact assessments, which we believe are overly prescriptive and are unlikely to deliver greater protection for consumers, as well as seeking prior authorisation from the supervisory authority for processes such as international transfers.
- Only supporting data breach notifications if the timescales and thresholds are appropriate, given the time it can take for organisations accurately to diagnose breaches.
- Pushing for a more proportionate system of fines, to avoid what we fear could lead to an over-compliance culture at the expense of investment in growth and innovation.

28. We support the Government taking a firm line on all of these issues to avoid locking in unnecessary regulations which deliver little for consumers or businesses and are hard to undo.

August 2012

Written evidence from Digital Policy Alliance

SUBMISSION TO THE HOUSE OF COMMONS JUSTICE SELECT COMMITTEE'S CALL FOR EVIDENCE ON THE PROPOSALS TO REFORM EU DATA PROTECTION LAWS

BACKGROUND

The Digital Policy Alliance (previously known as EURIM) brings together industry experts, observers from the civil service, professional bodies, charities and trade associations to help identify solutions to policy, regulatory and legislative problems impacting UK competitiveness, and to ensure that members' views and concerns are communicated to Ministers, Commissioners, Officials and Parliamentarians in London and Brussels.

The following response conveys the views of EURIM members to Questions 1 and 3 of the Justice Select Committee's call for written evidence focusing on the proposed General Data Protection Regulation. But many of the issues raised are also relevant to the proposed Directive. We would welcome an opportunity to discuss the issues raised in more detail.

Q1. *Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?*

1. We view the proposed General Data Protection Regulation (COM(2012)11) as an opportunity to update EU data protection laws and to address current problems. The steps taken to achieve greater harmonisation, clarity on applicable law and consistency of rules across EU Member States are cautiously welcomed, while the removal of notification requirements is seen as a step towards reducing current administrative burdens on data controllers. The move to clarify that applicable law for organisations should be based on the location of an organisation's main establishment in the EU is seen as a positive move forward, although the success of this approach will require consistency throughout the final Regulation.

2. Our members are concerned about the possibility of new barriers being introduced that could stifle business development. Data protection should be an enabler of the European Digital Single Market in which businesses based in a single member state play a leading role. The review should not lead to a legal framework that impedes the ability of companies based in the UK or in other member states to operate across Europe and internationally, or endangers Europe's digital development around innovative business models to meet the needs of UK citizens.

3. A balance must be found between protecting and securing the privacy of individuals and enabling data to be processed under a "principles—risk" based legal framework enforced by an appropriate and proportionate sanctions regime. The principles of the current Directive (95/46/EC) have been retained, but that balance may not be achieved because of the overall prescriptive approach being taken in the Regulation.

4. For example the lack of clarity on key definitions will create more legal and regulatory ambiguity, which could lead to different interpretations of the new rules preventing the processing of data. The broadening of the definition of personal data in Article 4 (1) is of particular concern as this could result in all information used by anyone, regardless of whether they are the data controller or not, being classed as personal data. This will not achieve the legal clarity as to when data is, or is not personal data. This "butterfly net" approach as suggested by the Commission appears intended to catch information under the Regulation without consideration of the context, the circumstances in which data is being processed, or whether the identification of a data subject is possible. A more granular approach is needed to acknowledge the importance of the context in which data is being processed as to whether identification of the data subject is possible. The proposed definition of personal data also makes it even more difficult for regulators to give such advice.

5. If all information is to be defined as personal data, this could mean that all the Regulatory rules, including on consent and data subject access requests would apply to network information processed to prevent online attacks. Given the Regulatory requirements of ensuring the security, integrity and availability of networks and systems that are vital to the provision on online services, the draft regulation should clarify that the processing of personal data necessary for ensuring network and information security is indeed permitted, as is recognised in Recital 39 of the proposed Regulation.

6. The proposed introduction of an "explicit" consent requirement could stifle business development by making the online experience for UK users cumbersome and slow. For example when purchasing goods or services online, users could be presented with multiple notices and have to navigate pages of information before gaining access to the actual goods or services. Such a situation could lead to individuals in the EU preferring easier-to-use services based outside the EU, thus impeding the future development of the European digital single market and the economic competitiveness of Europe in what is a global online marketplace.

7. The negative portrayal of profiling is also of concern. Profiling enables users to be offered relevant and useful search results and advertising, and many welcome this. The need is to enable genuinely informed user choice rather than discourage legitimate business practices that could and should be used to encourage UK and EU customers to use UK and EU based online services.

8. Another concern is the proposed reliance on delegated acts. This could lead to uncertainty on specific requirements in key areas, such as when data can be lawfully processed for legitimate business purposes (Article 6). Lack of clarity could lead to delays in decision-making on data privacy and security, thereby increasing the risk to citizens' data. The proposed use of delegated acts could lead to the introduction of technology-design mandates which would impact the technology neutrality of the legal framework and stifle innovation in areas where solutions need to continue to evolve to address new and emerging threats and risks to data.

9. The proposed changes to the rules under Article 6 of the Regulation could become a significant barrier to the ability of UK companies to process data for legitimate business purposes—a fundamental cornerstone of today's legal framework. For example the removal of the term "or by the third party or parties to whom the data are disclosed" will mean that those organisations that are not data controllers but also have a legitimate interest in processing data needed for business activities, including for the physical or electronic delivery of goods and services to UK consumers (and other member states), may no longer be able to do so.

10. The impact of increased administrative burdens and compliance costs, particularly on SMEs is unclear and needs further consideration. While it is understood that there are specific derogations granted to SMEs within the Regulation, there are concerns whether these are appropriate given that they currently do not take into account the risks to data being processed. For example, a specialist SME which processes highly sensitive data may be exempted from key requirements simply because of size.

11. Another area where the draft Regulation could impede the competitiveness of EU-based business operations is the proposal to introduce a right to data portability. We support the ability of individuals to be able to move their personal data between service providers but, given the focus of the proposed Regulation on data protection and given that industry has already developed policies, procedures and commercial practices to enable data portability, with no evidence of market failure, it is unclear as to why such a requirement is proposed.

12. There is no assessment of the possible impact and costs associated with the introduction of an explicit right to data portability. For example, if a user already has a contract with an online service provider relating to the storage of data for a period of time, what impact would an explicit right to remove that data at any time have on that contract? Such a "right" would also inhibit service providers from offering reduced rates for fixed term services (to ensure an adequate return in investment on the initial upfront costs of providing that service), thus reducing, rather than enhancing, consumer choice.

13. Finally, the potential economic implications to organisations of the proposed sanctions regime are of real concern. Enforcement mechanisms and meaningful sanctions are a necessary part of having an effective legal framework. However, arbitrary fines with sanctions of up to 2% of annual turnover are disproportionate to the penalties for non-data protection offences and could lead to bankruptcies. The proposed regime also appears to challenge the sentencing policy currently used by the UK Sentencing Council to set appropriate sentences, and should be reviewed.

14. We are concerned that unless these issues are addressed, any new data protection framework could be perceived by those outside Europe as a barrier to basing business operations within the EU, as well as impeding the investment and development of UK and EU business models and the innovation and growth of the EU digital single market.

Q2. *Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?*

15. The guiding principle of the UK negotiating position that the Regulation should be an instrument that "encourages economic growth and innovation" is both welcomed and supported by members.

16. We would have also liked to have seen the UK Government's negotiation strategy include concerns with the draft Regulation proposals regarding the definition of personal data, as well as the possible impact and feasibility of introducing "explicit" consent in all situations and the negative portrayal of profiling (see concerns raised above).

17. Nevertheless, overall key areas identified in the document's conclusion are seen as appropriate given the following concerns with regard to the proposals.

Support for the introduction of a transparency principle

18. While we agree with the UK Government's support for the introduction of a transparency principle, there are concerns that the introduction of prescriptive administrative requirements (for example the documentation requirements) for both controllers and processors may result in an increase in administrative burdens on organisations rather than a reduction. While we support greater transparency and the need to ensure that information is easy to understand and readily available, it is disappointing that the proposed administrative regime does not consider the need to assess the risks to data being processed in particular situations. We would welcome the UK Government including this in their negotiation strategy going forward.

Use of Delegated and Implementing Acts

19. There is real concern that the use of delegated acts in areas such as lawful business processing could reduce further development of innovative business models and growth of UK businesses. The use of delegated acts could also lead to the introduction of "design requirements" for technical measures in areas such as Privacy by Design and Data Portability which undermine the technology neutrality of the legal framework. It is important that the introduction of Privacy by Design does not result in design mandates which could impact the technology neutrality of the legal framework and stifle innovation in areas where solutions need to continue to evolve to address new and emerging threats and risks to data.

20. We are also concerned at the lack of any obligation for the Commission to consult stakeholders when drafting the details of delegated acts. This could result in a lack of checks and balances and the introduction of secondary legislation that changes the legal framework. Based on these concerns we urge the UK Government to call for removal of delegated acts in the articles related to Lawfulness of Processing, Privacy by Design and Default, Right to be Forgotten, Security of Processing, Administrative Sanctions, Responsibly of a Controller and Processor, Data Protection Impact Assessment, Prior Authorisation and Prior Consultation.

Overhaul of the Right to be Forgotten

21. We support the call for an overhaul of the proposed Right to be Forgotten given that there is already a deletion right under the Data Protection Directive. We support the latter and believe data subjects should have this ability, but there is a need to distinguish between the Right to be Forgotten and the Right to Erasure and clarity on how a Right to be Forgotten would work in practice. We need to avoid a situation where people think they have a Right to be Forgotten but the reality is different which could lead to confusion about citizens' legitimate rights, and impact on trust and confidence in data sharing (including where this is mandated by other Commission initiatives related to pan-EU public service delivery, such as the e-Identity Regulation).

22. It is not clear how this requirement will interact with other legislative requirements. For example, banks are not permitted to delete customer information that *might* be needed for investigations into criminal or terrorist activity. Banks have to be able to respond to requests from appropriate authorities for information on account holders; the standard retention time globally is 14 years.

23. The practical implications for data controllers of the introduction of a Right to be Forgotten and the potential impact this could have on data subjects are far from clear. Thus if a data subject makes a request to be forgotten and a data controller deletes the information related to that individual, would that deletion also include information related to the consent given, or not given, in relation to activities such as profiling? A situation could arise where data is sent which the individual has explicitly asked not to be sent, but for which there is no record of such a request because this was deleted as part of a Right to be Forgotten request.

Introduction of a Data Breach Notification

24. We support the introduction of an appropriate data breach notification requirement. However without complete harmonisation of the data security breach notification requirements in both the ePrivacy Directive and the proposed Data Protection Regulation, electronic communication providers are potentially subject to different reporting requirements in respect of different data sets. The introduction of a 24 hour deadline for notification is seen as not only unfeasible but conflicts with the ePrivacy Directive which is notification "without undue delay". If an incident does occur, the priority should be to ascertain the nature and extent of the attack and contain and investigate the breach, including protecting those at most risk. The requirement to report within 24 hours should therefore be deleted and replaced by "without undue delay"—the position under the current ePrivacy Directive.

25. It is also suggested that the approach taken in the ePrivacy Directive is followed by the introduction of a harm threshold criterion for determining the trigger for notification and when notification should be required. The definition of harm in the ePrivacy Directive should be introduced into the Data Protection Regulation to achieve this. This amendment would ensure that the Regulation is aligned with the requirements in the ePrivacy Directive and ensure harmonisation across EU laws.

Changes to Data Subject Access Requests

26. We support the UK Government's resistance to the introduction of free of charge access requests. The reality being faced by many companies today is a rise in data subject access requests which can result in significant operational and financial implications. The restoration of a small fee for subject data access requests has value as a deterrent against mischievous, irrelevant or time-wasting requests. A deterrent fee for abusive or costly requests would be justified because of the costs incurred although it is understood that all responses to requests have to follow a due process.

Introduction of more proportionate administrative penalties

27. We welcome the UK Government intention to call for changes in the proposed penalties structure. Our analysis of the draft Regulation reveals that the levels of penalties do not leave any room for administrative decisions by those imposing the fines. The proposed fines for breaches of the rules (ranging from 0.5% to 2%

of annual turnover) do not provide for any degree of proportionality to be taken into consideration, nor do they recognise the efforts and investment made by companies to be accountable in the event of a breach of the Regulations. It is also not clear what assessment has been made as to whether the proposed fine structure will have the desired effect and alter behaviour as a result of introducing these powers to DPAs.

28. While there is clearly a need to deal effectively with genuine wrong doing the current proposals are too prescriptive ("shall impose"), and offer the DPA too little discretion to look at the facts in the context of an incident. For example where a lesser penalty may be warranted because an organisation has taken steps to demonstrate accountability and an incident has still occurred. Such factors should be allowed for in the sanction regime.

29. Given that a key aim of the review of the legal framework is to introduce greater harmonisation on the rules and requirements for organisations under a "one stop shop" approach based on a single DPA, it is important that the Regulation is amended to ensure that only the lead competent supervisory authority can impose sanctions. The current wording on the Regulation particularly suggests that "each" data protection authority may impose sanctions. If this is not clarified it could result in organisations being fined by multiple authorities in different Member States. In light of the current fines being suggested this could lead to serious consequences for EU businesses of all size and shape if even the smallest fine was levelled multiple times.

August 2012

Printed in the United Kingdom by The Stationery Office Limited
11/2012 023538 19585