14 January 2011

Our ref: ICAEW Rep 06/11

Your ref: JUST-PRIVACY-CONSULTATIONS@ec.europa.eu

European Commission
Directorate-General Justice
Unit C3 – Data protection
B - 1049 Brussels

Dear Sir or Madam

CONSULTATION ON A COMPREHENSIVE APPROACH ON DATA PROTECTION IN THE EUROPEAN UNION

ICAEW is pleased to respond to your request for comments on *Consultation on a Comprehensive Approach on Data Protection in the European Union*.

Please contact me should you wish to discuss any of the points raised in the attached response.

Yours sincerely

Richard Anning
Head of IT Faculty, Technical Strategy Department

T +44 (0) 207 920 8635
F +44 (0) 207 920 8780
M +44(0)7787 280875
E richard.anning@icaew.com

ICAEW REPRESENTATION

ICAEW REP 06/11

CONSULTATION ON A COMPREHENSIVE APPROACH ON DATA PROTECTION IN THE EUROPEAN UNION

Memorandum of comment submitted in January 2011 by ICAEW, in response to European Commission consultation paper A Comprehensive Approach on Personal Data Protection in the European Union published in November 2010

Contents **Paragraph**

INTRODUCTION

1. ICAEW welcomes the opportunity to comment on the consultation paper *A Comprehensive Approach on Personal Data Protection in the European Union* published by the European Commission.

WHO WE ARE

2. ICAEW operates under a Royal Charter, working in the public interest. Its regulation of its members, in particular its responsibilities in respect of auditors, is overseen by the Financial Reporting Council. As a world leading professional accountancy body, we provide leadership and practical support to over 134,000 members in more than 160 countries, working with governments, regulators and industry in order to ensure the highest standards are maintained. We are a founding member of the Global Accounting Alliance with over 775,000 members worldwide.

3. Our members provide financial knowledge and guidance based on the highest technical and ethical standards. They are trained to challenge people and organisations to think and act differently, to provide clarity and rigour, and so help create and sustain prosperity. We ensure these skills are constantly developed, recognised and valued.

4. We are listed on the Register of Interest Representatives. Our registration number is 7719382720-34.

MAJOR POINTS

Support for the initiative

5. We welcome the Commission's efforts to update the Data Protection Directive. Given the pace of technological change since the Directive was originally drafted, it is timely to recognise the elements of the Directive which have worked effectively and look to improve areas which have been superseded by developments in technology.

6. In this regard, we feel that the technology-neutral approach taken in the original Directive has been shown to be the right approach. As such, we hope that the Commission continues to develop its work based on this principle and does not attempt to develop regulation which is specific to particular platforms and therefore will inevitably be overtaken rapidly by new technological developments.

7. Data protection is important to the growth of the digital economy. It underpins consumer and citizen trust in IT systems, the internet and the use of personal information for many social, economic and individual benefits. This does lead to an inherent tension, though, between the benefits of using and sharing personal information, and the need to restrict its use and flow. Any regulation needs to recognise this tension and find ways to protect personal information which do not unduly hamper or burden businesses in their operations and innovation.

8. We welcome the core ideas contained in the proposal, such as harmonisation and simplification. However, there is a significant challenge in translating these principles into practice which still needs to be addressed by the Commission. While there may be broad agreement on many of the principles outlined, much depends on the way in which these are translated into detailed rules. As it works through this process, we urge the Commission to continue to consult widely on its plans to enable input into specific proposals as they develop.

RESPONSES TO SPECIFIC QUESTIONS/POINTS

2.1.1: Ensuring appropriate protection for individuals in all circumstances

9. Technology has evolved in many ways and presents huge opportunities to use and share personal information which were not previously imaginable. All the indications are that this trend will continue into the future, leading to a need for a flexible and technology-neutral framework to manage the protection of personal data.

10. There is a natural tension between the benefits of protecting personal data and the benefits of the free flow of personal data. The use and sharing of personal data provides many economic, social and individual benefits and is the source of substantial innovation today. However, successful innovation is underpinned by consumer and citizen trust and an effective data protection framework is an important part of this.

11. The issues here are critical, complicated and very far-reaching. They illustrate some deep differences in the philosophical approaches to the concept of privacy contained in the arguments and concerns of different individuals and groups even within mainstream European social and business cultures, let alone more widely.

12. The protection of personal information, or privacy, is an intrinsically subjective topic, which makes objective analysis and societal generalisations challenging. As it is ultimately concerned with exercising choice about whether to keep information within a private domain or whether to share it with others, it will be strongly influenced by the psychology, social and political attitudes and personal experience of individuals. It is also dependent on the specific context of information sharing. Sharing medical information with a doctor, for example, is qualitatively different to sharing it with an insurance company.

13. The notion of privacy is strongly tied to the social and physical conditions of individuals and has changed substantially over time. Privacy also has a strong cultural basis. It is largely drawn from Western political and philosophical traditions of individual liberty and Asian and African cultures have much less of a tradition in this area

14. These factors make it very difficult to formulate a coherent set of data protection rules for personal data and to ensure the consistent application of such rules in all circumstances. The matters mentioned in the Commission's Communication COM(2010) 609 final are by no means comprehensive. Other issues that need to be taken into account include:

14.1. How we define privacy and how we differentiate between the different scenarios where we see privacy concerns. Our own researches have outlined many different concerns and it may be helpful to distinguish between different types of privacy, so that the debate around benefit, harm and action can be more nuanced. There are substantial differences, for example, between the building and use of structured databases of personal information and the voluntary disclosure of unstructured personal data on the internet. Professional Daniel Solove has developed a typology for privacy and further thinking along these lines may be useful (see, for example, Solove's book 'Understanding Privacy', web link http://docs.law.gwu.edu/facweb/dsolove/Understanding-Privacy)

14.2. How to define the individual, economic and social benefits of privacy. While many surveys, such as the annual survey by the UK Information Commission (http://www.ico.gov.uk/~/media/documents/library/Corporate/Research_and_reports/annual_track_2010_individuals.ashx), suggest that individuals continue to have high levels of concern around personal information, there are divergent views of the benefits of privacy to an individual. Furthermore, the wider social and economic benefits of privacy, for example in supporting trusting relationships, remain under-explored.

14.3. How to compare the benefits of privacy with other interests. Finding ways to balance the interests of consumers and businesses, or citizens and governments, remain difficult to achieve in practice and further debate is needed.

14.4. How privacy can develop global meaning given its cultural groundings. This is a significant practical issue for businesses as well as a challenging one in theory. As the economy and society continue to become more globally connected, this challenge will also increase.

15. We should be pleased to participate in any activity organised by the Commission as part of its consideration of such issues with a view to developing greater coherence in the application of data protection principles and rules in the future.

2.1.2: Increasing transparency for data subjects

16. A "general principle of transparent processing" will not really take us any further forward, except perhaps as a statement of the background to taking more practical steps. The Commission should place emphasis on the much more practical objectives of introducing specific obligations for data controllers on the nature of the information to be provided to those from whom they are collecting data and drawing up legally binding templates for privacy information notices.

17. There is a risk, though, that such requirements become unduly burdensome on businesses. The dangers relating to personal information vary substantially across businesses depending on the business model adopted and the amount and sensitivity of personal data held. The uses of personal data will also change as technology evolves and individuals adopt new applications or services.

18. As a result, detailed requirements in this area need to take account of these differences to ensure that the administrative burden is minimised, reflects the different degrees of risk attached to different types of business activities in this area and can respond effectively to the fast changing environment.

19. Detailed requirements also need to ensure that the information provided to consumers is simple and understandable. There is a balance to be struck as high levels of transparency and control are not necessarily easy to understand and exercise. While a business may seek to give users very granular control over how their personal data is used and shared, this may not be what users really want. Traffic light systems, as used in food labelling, provide one example of communicating risk-based information to consumers in a simple and comparable manner which could present some lessons for the area of data protection.

20. Regarding the proposal for a breach notification law, this is a practical proposal on the achievement of which the Commission should place priority. However, such a law needs to be framed carefully regarding aspects such as the definition of a data breach and the circumstances in which notification is required. There is substantial experience of the working of data breach notification laws in the USA and we suggest that the Commission look in considerable detail at the evidence gained on the practical operation of such laws as it progresses this proposal.

2.1.3: Enhancing control over one's own data

21. We support the Commission's efforts to improve the modalities for the exercise of rights of access, rectification, erasure or blocking, However, this section identifies some of the most intractable problems relating to the implementation of data protection, even when the relevant principles are quite clearly expressed. It is questionable whether "strengthening" the principles would prove to be particularly effective.

22. For example, the Commission's proposals include clarifying the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. It is a little disturbing to read that this principle, which seems to be expressed quite clearly and to be quite easy to understand, needs to be "clarified". We do note that, perhaps,

the principle is only implicit in the wording of Article 6 of Directive 95/46 EC, rather than stated explicitly. The main problem seems to us, however, not that the principle is unclear but that the existence of the principle does not achieve the required or expected result.

23. There are philosophical issues around the retention and use of personal data which need to be considered. As the Commission rightly states, data may be retained for legitimate purposes, limiting a 'right to be forgotten'. Therefore, detailed consideration is required concerning what are 'legitimate purposes' , including the proper balance (i) between personal data privacy and the legitimate commercial exploitation of personal data and (ii) between personal data privacy and the better definition of proper limits on the use of personal data in the public sector.

24. In the case of the public sector, consent may not be the appropriate basis for making use of the information and therefore a 'right to be forgotten' may be limited to promote broader public interests. In particular, retaining and sharing data relating to crime and security could prevent future incidents happening and help to detect criminals or terrorists.

25. There are also practical issues. We consider that one of the main difficulties in giving effect to this principle is the extent to which personal data nowadays are copied, extracted from users' web browsers, sold and otherwise distributed electronically, whether legitimately and with full and informed consent or otherwise. We believe that the Commission should concentrate on establishing the extent to which it is still possible in practical terms to achieve this principle and on helping to establish effective ways of enforcing it.

26. A 'right to be forgotten' can only ever be a very limited right. It is evidently still not clear to many people that anything posted on a social web site, and indeed most data or data objects such as photographs posted on most web sites, are irretrievably public in the sense that they are no longer under the control of the original copyright owner and can be copied limitlessly by others. In most cases, the original copyright owner will in any case, wittingly or unwittingly, have permitted such copying, to some extent at least, as an aspect of the contract for the use of the service.

27. In this context, it may again be helpful to distinguish between different types of data and scenarios. For example, where a business or individual has provided data to a cloud provider as part of a serviced contract, it should be possible to ensure the complete deletion of the specified data. However, where a piece of data has been voluntarily shared over the internet, such erasure is more difficult. There seems no way of achieving the erasure of serial copying of such data objects, once they have been posted on a web site, however much the original copyright owner might desire such erasure. We believe that the Commission's concern should be to ensure only what it is possible to ensure, namely that the original hosting site for the data objects should be required to delete them from the original copyright holder's area of the site and, after a reasonable time, from the archive of that part of the site, at the request of the data subject.

28. Data portability is desirable as a means of encouraging competition between hosting sites, but the technical feasibility of achieving full data portability across different platforms designed in different ways is open to considerable question and seems of little value at the margins, bearing in mind that many users may regard a lot of the relevant data as ephemeral. To that extent, it seems worthwhile for the Commission to promote data portability, but not really worth the Commission spending a lot of resources trying to ensure it.

29. When developing detailed requirements, the Commission should also consider the potential burden on businesses, especially on small businesses, in complying with the regulations and meeting requests from individuals regarding their data.

2.1.4: Raising awareness

30. Many individuals still seem to be unaware of many of the risks attached to the widespread sharing of their personal information. They also fail to take basic steps regarding the protection and security of their information. As a result, there is a clear need for awareness-raising activities across citizen and consumer communities.

31. The suggestion of introducing legal obligations to carry out awareness-raising activities, though, needs a lot of detailed consideration of (i) the particular agencies or organisations which ought to be so obliged and (ii) the legal definition of "awareness-raising activities", which is a particularly nebulous term in ordinary language.

2.1.5: Ensuring informed and free consent

32. We consider that the issue of consent is at the heart of the philosophical and practical problems associated with personal data protection.

33. As the Commission consultation document rightly says, "it is not even clear what would constitute freely given, specific and informed consent to data processing, such as in the case of behavioural advertising, where internet browser settings are considered by some, but not by others, to deliver the user's consent."

34. Concerns in this area are being driven particularly by behavioural advertising, which bases advertising activities on the detailed tracking of individual internet activities. Although the data may not always be personally identifiable, these activities have generated significant concerns about the degree of consent given, the amount of data captured and the sophistication of the analysis and segmentation of individuals. However, this type of advertising has driven many free internet services and advocates argue that this type of advertising is a positive development. As it targets advertisements much more accurately than has previously been possible, it potentially benefits individuals, as they are likely to be getting advertisements which are of more interest to them, as well as being more effective for advertisers. Therefore, the benefits of technological capability again need to be balanced against the risks to individuals and the harm that could be done to them through the unwanted collection and use of their personal information.

35. While there is this degree of disagreement in connection with matters as central to the issue as this, particularly when there is little general understanding of the technical aspects of the issue, there seems little chance of gaining quick agreement on ways of clarifying and strengthening the rules on consent. We therefore do not believe that the issues can be fully resolved in relation to the legal requirements of personal data protection unless and until the nature and scope of "consent" in today's society has been much more specifically defined than when the concept was first incorporated into the data protection principles recognised in European law. We consider that, before the Commission seeks to clarify the rules, let alone seeks to strengthen them, it has an important role to play in elucidating and seeking to reconcile the different attitudes in today's society towards the nature and scope of consent in relation to the use of personal data. We should be pleased to help in this process. We also suggest that the Commission closely consider the evidence relating to how effectively the ePrivacy Directive has been implemented and how significant has been its impact, as this Directive covers questions of consent around the internet.

2.1.6: Protecting sensitive data

36. We agree with this proposal.

2.1.7: Making remedies and sanctions more effective

37. No comment.

2.2.1: Increasing legal certainty and providing a level playing field for data controllers

38. We support this proposal, which would achieve greater legal certainty across the different jurisdictions of the EU and would therefore be helpful both to individuals and to businesses. However, further detail is required as to what this means in practice.

2.2.2: Reducing the administrative burden

39. We again support the objective of simplifying and harmonising data protection rules.

2.2.3: Clarifying the rules on applicable law and Member States' responsibility

40. No comment.

2.2.4: Enhancing data controllers' responsibility

41. The volumes of personal data processed by most small businesses and micro-businesses are likely to be low and the scope of the data is likely to be limited. We therefore consider that it is very important to ensure that such businesses, while of course remaining fully subject to the law in respect of personal data protection and to the application of the data protection principles, are exempted from unduly detailed bureaucratic requirements more obviously appropriate to larger organisations, such as the mandatory appointment of an independent Data Protection Officer.

2.2.5: Encouraging self-regulatory initiatives and exploring EU certification schemes

42. We recognise that regulation is only one aspect of improving the protection of personal information and there are important roles for the market and self-regulation initiatives in improving standards in ways which are appropriate to specific businesses and industries.

43. There will clearly be a role for certification and 3rd party audits of business practices. However, we suggest that the Commission focus its resources and efforts on establishing the right overall framework for data protection and encourage schemes such as certification to follow, if it becomes more clear that this would be the most appropriate course.

2.3: Revising the data protection rules in the area of police and judicial cooperation in criminal matters

44. In principle we agree with the objective to extend data protection rules to these areas.

2.4.1: Clarifying and simplifying the rules for international data transfers

45. We support these proposals. The core EU data protection elements, as well as being of value in relation to international agreements, could be of help in defining such matters as the essential requirements for consent to processing, as discussed above.

2.4.2: Promoting universal principles

46. We support these proposals.

47. High legal and technical standards, while necessary, are not in themselves sufficient to ensure the security or the privacy of data in the absence of a proper and adequate understanding of the issues by users of personal data, at whatever level within an organisation, and effective ongoing education and training for personnel at all levels in relation to these issues. We therefore consider that the EC should seek to promote the development of high standards of data management, as well as high legal and technical standards, in third countries and internationally, as well as within the EU itself.

48. This is particularly important given the global nature of many businesses today:

48.1. Personal data are under the practical control of many different parties, not just the organisation which owns the data. Although the organisation remains responsible for the

data and needs to ensure any third party suppliers comply with laws, it makes the process more complex and risky.

48.2. Personal data are under the jurisdiction of many different regimes throughout the lifecycle as data moves between locations which may be much less strict, making compliance complex and expensive.

49. Furthermore, different cultures continue to have very different conceptions of privacy. Employees may have different views as to privacy and apply different standards of care than would be expected in other countries. Customers are also likely to have different expectations regarding privacy depending on where they are situated.

50. As a result, a global business is likely to need a sophisticated and nuanced view of privacy which takes account of these cultural and legal differences. However, where international institutions can work towards a degree of harmonisation and standardisation, this is likely to be highly beneficial to businesses. Given the experience of the EU in this area, it is helpful for it to take a leading role.

2.5: A stronger institutional arrangement for better enforcement of data protection rules

51. If this would achieve greater legal certainty across the different jurisdictions of the EU, it would be helpful both to individuals and to businesses.

52. We believe that transparency in the operation of public bodies is always beneficial. We agree that the Article 29 Working Party, or whatever body might complement or supersede it, ought to become more transparent in its operations.

E richard.anning@icaew.com