BCS, The Chartered Institute for IT
Consultation Response to:

‘A Comprehensive Approach to Personal Data Protection in the European Union’
Dated: 15 January 2011
This page is left deliberately blank.
BCS, The Chartered Institute for IT

The Institute promotes wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for IT, we serve over 70,000 members including practitioners, businesses, academics and students, in the UK and internationally. We deliver a range of professional development tools for practitioners and employees.

A leading IT qualification body, we offer a range of widely recognised professional and end-user qualifications.

www.bcs.org
The Institute observes that in general, the document makes numerous assertions backed by references to external data, but apart from referencing the Lisbon Treaty, does not present an argument to support the stated conclusions and recommendations.

2 Key Objectives of the Comprehensive Approach on Data Protection

2.1 Strengthening individuals’ rights

2.1.1 Ensuring appropriate protection for individuals in all circumstances

The Commission will consider how to ensure a coherent application of data protection rules, taking into account the impact of new technologies on individuals’ rights and freedoms and the objective of ensuring the free circulation of personal data within the internal market.

Comments:

The application should be not only coherent, but also consistent and we need to understand whether there is an expectation of strengthening or weakening of rights in order to achieve this outcome. The objective of ‘ensuring the free circulation of personal data within the internal market’ suggests a desire to circumvent aspects of data protection rules or specific implementations in member states.

2.1.2 Increasing transparency for data subjects

The Commission will consider:

• Introducing a general principle of transparent processing of personal data in the legal framework;
• Introducing specific obligations for data controllers on the type of information to be provided and on the modalities for providing it, including in relation to children;
• Drawing up one or more EU standard forms (‘privacy information notices’) to be used by data controllers.

The Commission will examine:

• The modalities for the introduction in the general legal framework of a general personal data breach notification, including the addressees of such notifications and the criteria for triggering the obligation to notify.

Comments:

The text calls for the use of ‘clear and plain language’, yet the stated objectives of the Commission are unclear, and the wording of these objectives is confusing. The concept of EU standard forms is worrying, since this is likely to result in standardised consent notices which cover a broader range of processing than is necessary, and hence erodes privacy outcomes by contradicting the objective of minimisation stated in section 2.1.3.

Whilst the intention of a general personal data breach notification may be of value, such a framework may struggle in the context of varying national data protection implementations and associated penalties or the appetites of individual Commissioners to enforce those
penalties. There may be value in imposing a consistent method and penalty framework, but the Institute accepts that this topic is substantial and would have deep and broad implications for the management of data protection across Europe.

2.1.3 Enhancing control over one’s own data
The Commission will therefore examine ways of:
• strengthening the principle of data minimisation;
• improving the modalities for the actual exercise of the rights of access, rectification, erasure or blocking of data (e.g., by introducing deadlines for responding to individuals' requests, by allowing the exercise of rights by electronic means or by providing that right of access should be ensured free of charge as a principle);
• clarifying the so-called ‘right to be forgotten’, i.e. the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. This is the case, for example, when processing is based on the person's consent and when he or she withdraws consent or when the storage period has expired;
• complementing the rights of data subjects by ensuring ‘data portability’, i.e., providing the explicit right for an individual to withdraw his/her own data (e.g., his/her photos or a list of friends) from an application or service so that the withdrawn data can be transferred into another application or service, as far as technically feasible, without hindrance from the data controllers.

Comments:
The Institute welcomes the concept of a ‘right to be forgotten’ and the associated legal and technological requirements to make that right a reality. For this approach to succeed, the Commission will need to take steps to ensure that Data Controllers properly declare the jurisdiction under which the data is held, and to consider the implications of enforcement where that jurisdiction sits outside the EU.

2.1.4 Raising awareness
The Commission will explore:
• the possibility for co-financing awareness-raising activities on data protection via the Union budget;
• the need for the opportunity of including in the legal framework an obligation to carry out awareness-raising activities in this area.

Comments:
The Institute welcomes the intention to continue to raise awareness of data protection, but urges that this must be coupled with actions to catalyse change in behaviour and ensure that those changes become embedded in normal practices: it is not enough just to raise awareness if any behavioural change is to be adopted and maintained over time. Clear timetables and benchmarking activities should also be established to ensure that the effectiveness and value for money of awareness activities can be monitored.
2.1.5 Ensuring informed and free consent
The Commission will examine ways of clarifying and strengthening the rules on consent.

Comments:
The Institute welcomes the intention to clarify and strengthen the rules on consent, and observes that for this to be effective, individuals need to be empowered with tools that allow them to prove what consent was given and when, since in most cases individuals do not have an effective method to record that consent, and thus the data controller’s records are the only evidence of consent that is available in the event of a dispute. It is also important to ensure that there are adequate mechanisms in place to record any revocation of consent.

2.1.6 Protecting sensitive data
The Commission will consider:
• whether other categories of data should be considered as ‘sensitive data’, for example genetic data;
• further clarifying and harmonising the conditions allowing for the processing of categories of sensitive data.

Comments:
Whilst the Institute welcomes the intention to harmonise the conditions for the processing of categories of sensitive data, it should be noted that there is a very wide range of data types that may be considered ‘sensitive,’ and that whether or not a specific data type is sensitive may depend upon context. There is a concern that over-prescriptive specifications for processing may in fact undermine the protection of sensitive data.

2.1.7 Making remedies and sanctions more effective
The Commission will therefore:
• consider the possibility of extending the power to bring an action before the national courts to data protection authorities and to civil society associations, as well as to other associations representing data subjects’ interests;
• assess the need for strengthening the existing provisions on sanctions, for example by explicitly including criminal sanctions in case of serious data protection violations, in order to make them more effective.

Comments:
The document should clarify whether it is the Commission’s intention to explore the role of class action lawsuits. The Institute observes that such actions may result in a reduced appetite for breach notification if organisations then face class actions as a consequence of those notifications.
2.2 Enhancing the internal market dimension

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

The Commission will examine the means to achieve further harmonisation of data protection rules at EU level.

Comments:
The Institute is concerned that harmonisation in the interests of promoting the internal market may dilute the general level of protection afforded.

2.2.2 Reducing the administrative burden

The Commission will explore different possibilities for the simplification and harmonisation of the current notification system, including the possible drawing up of a uniform EU-wide registration form.

Comments:
The Institute would support the aim of a reduction of any administrative burdens which do not in themselves provide added protection. However, notification can be beneficial where the information provided supports the transparency of processing. The Institute believes that notifications should in general be published on the internet.

2.2.3 Clarifying the rules on applicable law and member States’ responsibility

The Commission will examine how to revise and clarify the existing provisions on applicable law, including the current determining criteria, in order to improve legal certainty, clarify member States’ responsibility for applying data protection rules and ultimately provide for the same degree of protection of EU data subjects, regardless of the geographic location of the data controller.

Comments:
The Institute wishes to point out that the effective clarification of applicable law requires the establishment of binding international agreements and cannot be unilaterally defined by the Commission. The Commission needs to engage with foreign governments to ensure that the rights of EU citizens whose data are processed in third countries are preserved.

2.2.4 Enhancing data controllers’ responsibility

The Commission will examine the following elements to enhance data controllers’ responsibility:

- making the appointment of an independent Data Protection Officer mandatory and harmonising the rules related to their tasks and competences31, while reflecting on the appropriate threshold to avoid undue administrative burdens, particularly on small and micro-enterprises;
- including in the legal framework an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance;
- further promoting the use of PETs and the possibilities for the concrete implementation of the concept of ‘Privacy by Design’.
Comments:
The Institute feels that there are risks in delegating supervisory responsibilities to Data Protection Officers (DPO’s) who may be perceived to have a conflict of interests. It is not clear what mechanisms are being proposed to ensure their independence. The Institute considers that data controllers that are required to employ DPO’s should also be required to notify and publish details of their processing of personal data.

2.2.5 Encouraging self-regulatory initiatives and exploring EU certification schemes
The Commission will:
• examine means of further encouraging self-regulatory initiatives, including the active promotion of Codes of Conduct;
• explore the feasibility of establishing EU certification schemes in the field of privacy and data protection.

Comments:
The Institute supports the concept of increased self-regulation and certification, provided that adequate enforcement measures are retained and subject to independent regulation.

2.3 Revising the data protection rules in the area of police and judicial co-operation in criminal matters
The Commission will, in particular:
• consider the extension of the application of the general data protection rules to the areas of police and judicial cooperation in criminal matters, including for processing at domestic level while providing, where necessary, for harmonised limitations to certain data protection rights of individuals eg concerning the right of access or to the principle of transparency;
• examine the need to introduce specific and harmonised provisions in the new general data protection framework, for example on data protection regarding the processing of genetic data for criminal law purposes or distinguishing the various categories of data subjects (witnesses; suspects etc) in the area of police cooperation and judicial cooperation in criminal matters;
• launch, in 2011, a consultation of all concerned stakeholders about the best way to revise the current supervision systems in the area of police cooperation and judicial cooperation in criminal matters, in order to ensure effective and consistent data protection supervision on all Union institutions, bodies, offices and agencies;
• assess the need to align, in the long term, the existing various sector specific rules adopted at EU level for police and judicial cooperation in criminal matters in specific instruments, with the new general legal data protection framework.

Comments:
The Institute supports the concept of harmonising the application of data protection rules in the areas of police and judicial co-operation, but will need to see the detailed proposals before forming a view. The Institute points out that any consideration of police and judicial co-operation will need to include the measures for disclosure of such data to and any subsequent processing in, third countries.

2.4 The global dimension of data protection
2.4.1 Clarifying and simplifying the rules for international data transfers
The Commission intends to examine how:
• to improve and streamline the current procedures for international data transfers, including legally binding instruments and ‘Binding Corporate Rules’ in order to ensure
a more uniform and coherent EU approach vis-à-vis third countries and international organisations;
• to clarify the Commission’s adequacy procedure and better specify the criteria and requirements for assessing the level of data protection in a third country or an international organisation;
• to define core EU data protection elements, which could be used for all types of international agreements.

2.4.2 Promoting universal principles
The Commission will:
• continue to promote the development of high legal and technical standards of data protection in third countries and at international level;
• strive for the principle of reciprocity of protection in the international actions of the Union and in particular regarding the data subjects whose data are exported from the EU to third countries;
• enhance its cooperation, to this end, with third countries and international organisations, such as the OECD, the Council of Europe, the United Nations, and other regional organisations;
• closely follow up the development of international technical standards by standardisation organisations such as CEN and ISO, to ensure that they usefully complement the legal rules and to ensure operational and effective implementation of the key data protection requirements.

Comments:
The Institute agrees that the current procedures for the regulation of cross-border disclosure of personal data are to a large extent cumbersome, bureaucratic and ineffective. However, this is an area in which the Commission should not act unilaterally, but should aim to negotiate and aim to establish binding international instruments and the development and observation of international standards.

2.5 A stronger institutional arrangement for better enforcement of data protection rules
The Commission will examine:
• how to strengthen, clarify and harmonise the status and the powers of the national Data Protection Authorities in the new legal framework, including the full implementation of the concept of ‘complete independence’;
• ways to improve the cooperation and coordination between Data Protection Authorities;
• how to ensure a more consistent application of EU data protection rules across the internal market. This may include strengthening the role of national data protection supervisors, better coordinating their work via the Article 29 Working Party (which should become a more transparent body), and/or creating a mechanism for ensuring consistency in the internal market under the authority of the European Commission.

Comments:
The Institute considers that whilst the Article 29 Working Party should continue to have an important role to play, there should be an increased emphasis on the involvement of industry, academic and professional bodies in the future development and enforcement of data protection rules.

End