289 – 293 High Holborn, London
ETI ID Number: 85696601933-11

Bar Council of England and Wales
Brussels Office

Ave des Nerviens 85
B-1040 Brussels
Belgium
Tel: 02/230 48 10
Fax: 02/230 45 96
e-mail: evanna.fruithof@barcouncil.be

Response of the Bar Council of England and Wales to the European Commission's consultation on its comprehensive approach to Personal data protection in the European Union

Introduction

1. The General Council of the Bar of England and Wales ("the Bar Council") represents the interests of some 15,000 barrister members. As the Bar's governing body, its role is to promote and improve the function of the Bar and its services to its clients; and to represent the interests of the Bar on all matters relating to the profession, including on changes to law or procedure.

2. This response has been prepared by the Law Reform Committee, with the support of the European Committee, of the Bar Council. We welcome the opportunity to comment on the European Commission's comprehensive approach to personal data protection in the European Union.

Comments on the Commission's plans

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.**

3. We endorse the Commission's aim to develop a comprehensive and coherent approach to data protection, designed to protect personal privacy in the modern world, where new technologies for the collection, analysis, storage and sharing of information have transformed personal information into a powerful and valuable commodity.

4. However, we think it is crucially important that, in re-designing the data protection regime, the Commission is always guided by the fact that the protection of personal data is an aspect of the right to privacy. The reason that data protection rules

are important is because they are a key means for individuals to protect information that is personal to them. Data protection cannot simply be about technology; it cannot be formulaic, technical, rule-based. The right to protection of personal data must first and foremost be seen as the right to protection of personal privacy. In case the contrary should be suggested, we see no conflict between the protection of individual rights on the one hand and free circulation of data within the market on the other. The internal market provides an opportunity to ensure individual rights enjoy the highest standards of protection throughout the territory of the EU, with best practice spreading among the Member States. Public confidence that their data privacy rights will be respected when acting as consumers of transboundary goods and services is essential to promoting trade between Member States.

5. The right to privacy of personal information is important as it may play a substantive role in determining how to apply the provisions of the Directive to a number of situations where the rights of individuals are not at risk, and it may caution against any interpretation of the same rules that would leave individuals deprived of protection of their rights.

6. The consultation discussion rightly begins with the concept of "personal data". It is our view that the definition of "personal data" should remain broad and that the concept of identifiability should remain as the touchstone of the definition. The breadth of the concept is appropriate to safeguard the wide range of personal information that is processed. It also properly allows for data protection rules to apply to new types of information.

7. The Commission should ensure that the understanding of "personal data" is harmonised across Member States. For example, the ambit of "personal data" has been narrowed by the court in the United Kingdom, and although the UK's Data Protection Authority, the Information Commissioner, has taken steps to counteract that narrowing, his efforts have not been wholly successful.

8. The legislation should be framed in such a way that implementation by Member States is based on giving effect to the principles animating the Directive, and that data protection does not simply become a check-box exercise. If the Commission concludes that divergence in the manner and effectiveness of Member State implementation is itself a factor contributing to inadequate protection for data subjects, it should actively consider replacing the Directive with a Regulation.

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.

9. We support the introduction of a general principle of transparent data processing, which places a duty on data controllers to tell individuals:

a) whether the data controller is collecting, processing or storing[1] personal data;
b) how the collecting, processing or storing is happening;
c) who is doing the collecting, processing or storing;
d) why the data is being collected, processed or stored;
e) how long the information will be processed or stored;
f) that individuals have the right to access, rectify or delete data;
g) how those rights can be exercised;
h) who the competent data protection supervisory authority is and its contact details.

The adoption of a general principle will emphasise, strengthen and enlarge upon those rights already afforded data subjects through Articles 10 and 11 of the Directive. It will also help to provide clarity for data controllers.

10 In the online environment, the transparency principle will require that providers of authenticated services (ie services which can only be used by a user who has "signed-in" or otherwise identified themselves) be open about how, why and for how long the user's personal information will be processed. It should also require providers to explain various levels of privacy in the use of services (eg users should be told about privacy settings on social networks which prevent information from being accessed by the general public; or privacy settings on search engines which prevent results being intercepted by third parties or search histories from being stored).

11. We also support the adoption of standard form privacy information notices, drafted in clear, plain language and as simply and briefly as possible. It is, however, necessary to be realistic about how much privacy information notices can achieve. Users of the internet expect their use to "flow" simply and easily and to be able to access information/services without the interruption of having to read documents about privacy (or security or even terms and conditions). The suspension of the "flow" for a yes/no tick-box in relation to privacy will not mean that the privacy information has been read. Privacy information notices are principally aimed at:

a) ensuring that the data controller has thought about privacy and can be held to the privacy standards it professes to maintain;
b) providing information to those who are interested in/worried about the privacy of their personal information.

12. A more important tool for protecting personal information of internet users is encouraging privacy by design, so that users' privacy settings are automatically set to give the greatest protection but to allow users to choose lower privacy settings. As

[1] Although storage of data is included in the broad definition of "processing", the general public is unlikely to understand that processing includes storing. The retention and storage of personal information is one of people's the key concerns. Any principle (and any obligations or standard forms flowing from that principle) should therefore explicitly mention retention/storage of data.

already mentioned, the effect of privacy settings on who can access information and how information is collected, processed and stored should be made clear to users – this element of privacy by design dovetails with the transparency principle.

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.

13. We agree that there should be a mandatory breach notification requirement. There is no obvious reason why mandatory breach notification should be limited to one sector (as it currently is in the e-Privacy Directive), particularly given the range of information held by service providers who process sensitive personal data (eg online banks and insurers, online providers of health services) and the fact that experience has shown that organisations such as banks and public bodies have been equally responsible for serious data security breaches.

14. There is also a significant risk that the rules in Member States relating to mandatory notification will begin to diverge significantly. Some Member States already have general mandatory notification requirements, and there is nothing to prevent Member States implementing the terms of the e-Privacy Directive more widely than it is drafted, to include a broader range of data controllers. Accordingly, in order to promote harmonisation and to encourage better data security practices, a mandatory breach notification requirement should be introduced.

15. There are various modalities for mandatory breach notification requirements. In Germany, for example, the reporting obligation is confined to circumstances where the data breach concerns sensitive personal data, certain other prescribed categories of sensitive data and any data which puts the relevant data subject at "imminent risk". The scheme requires simultaneous reporting to both the data protection authority and individuals. In Ireland, recent recommendations have been made for a broad mandatory reporting requirement to be adopted, in which almost all breaches would be reportable to the Office of the Data Protection Commissioner.

16. There are advantages and disadvantages in both a wide and a narrow reporting requirement. A narrow requirement, limited perhaps on the basis of severity of breach or of potential harm, would help to minimise the potential flood-gate effect of mandatory reporting. It might also prevent the public from being unnecessarily alarmed by sensationalist media reports in respect of relatively minor incidents. However, unless the required degree of harm for reporting purposes is clearly defined, there is a risk that the concept of harm will become subjective, and that serious breaches may slip though the net. A broad requirement, encompassing even the most minor data breaches, has the benefit of being simple to understand and enforce. However, it may swamp the data protection supervisory authority with reports of insignificant incidents.

17. In our view, a mandatory reporting requirement should not be limited only to sensitive personal information. It may be prudent to limit the requirement on the basis of the severity of the breach, but any limiting criteria should be very clearly defined. The requirement should be to inform both the data protection supervisory authority and the affected individuals simultaneously, so that the data subjects are informed of the breach as soon as possible, rather than this being deferred pending the outcome of an investigation.

The Commission will 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

18. We agree that the principle of data minimisation needs to be strengthened. The basic principle, from initial acquisition of data through every stage of subsequent processing, should be that the personal data gathered and processed must be the **minimum necessary** to achieve the object of the operation. That is a facet of the principle of proportionality. Minimisation should be designed into all automated processing, and practised in all human processing through clear instructions and guidance to operatives, so that only those data fields strictly relevant to the particular operation being undertaken are consulted and acted upon.

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

19. In our experience, the right to make subject access requests is well used in the United Kingdom, but other rights are under-utilised. In particular, the right to compensation under s13 of the Data Protection Act 1998 has not been well used, even though the entitlement to compensation for damage for distress by reason of contravention of the data protection principles is, in theory, a strong right and one

which could be used far more extensively to protect privacy. Part of the difficulty may be that the defence under the s13(3) DPA to the claim for compensation is that the data controller took such care to comply with the requirements concerned as was reasonable in all the circumstances. This might be construed as providing a more generous defence than Art 23.2 of the Directive: that the data controller was not responsible for the event giving rise to the damage. The Commission may wish to consider whether "responsible" should be replaced with clearer language defining the scope of the data controller's defence

20. Alongside any awareness-raising campaigns supported by the Commission, it should also ensure that Member States properly implement the rights available to data subjects in the Directive.

21. Awareness-raising should highlight the fact that data protection really means the safeguarding of personal information and should stress the link between privacy and data protection. Any awareness-raising activities aimed at the general public should be as simple and direct as possible. Awareness-raising among data controllers is also required, so that their obligations are explained in an easily understandable way and so that they appreciate that the data protection duties stem from the need to protect privacy.

22. Although we strongly support the need for awareness-raising activities, we do not agree that a positive legal obligation to carry out discrete awareness-raising activity is either apt or workable. However, we would support a compromise approach under which the Member State authorities are required to carry out their functions in a way that promotes public awareness-raising.

The Commission will examine ways of **clarifying and strengthening the rules on consent.**

23. We agree that the rules on consent need to be clarified and strengthened. The definition of consent in the Directive leaves open the question of whether the "opt-out" approach to consent is required, or whether opt-in is sufficient - this should be clarified.

24. Art 13 of the e-Privacy Directive allows for "soft opt-in" - ie where contact details are supplied in the context of a sale of a product or service, those details can be used for direct marketing "provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use." This gives clearer guidance than does the Directive, and has broadly been welcomed by organisations that provide goods or services online. It provides a good basis from which to reform the Directive.

25. Any reconceptualisation of consent needs to achieve a balance between clarifying what the requirement actually means and taking a pragmatic approach which recognises

that individuals may not always want or need to exercise explicit consent to certain types of processing. However, internet browser settings are not a reliable indication of consent and the Directive should make this clear.

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.

26. We consider that personal data is sensitive when the data subject is likely to experience particular damage or distress if the information were improperly or insecurely processed.

27. Of particular importance to the effective protection of sensitive data is a sufficiently broad interpretation of the concept of "processing". For example, Article 8(3) of the Directive limits the processing of sensitive data (in practice, medical data) to certain purposes and to "a health professional subject... to the obligation of professional secrecy or... another person also subject to an equivalent obligation...". "Processing" includes not just active use or dissemination of the data but also their consultation so as to glean information from their contents. Thus it is plainly inconsistent with Article 8 to permit medical information to be consulted and read by the general public without the data subject's explicit consent. Any interpretation of the Directive which held such activity by the public not to be "processing" the data would evade the plain intention of the Directive to confer a high level of privacy on this kind of information.[2] The legislation should make this broad interpretation of "processing" clear beyond peradventure.

28. Genetic data is closely allied with medical data – it is usually obtained through a medical process and it contains information about health. In the United Kingdom, there is particular concern that genetic data is properly and securely dealt with. The Human Tissue Act 2004 requires "appropriate consent" (ie active consent) for the lawful storage and use of human tissue and also creates a criminal offence of DNA theft, with penalties of up to three years imprisonment for failing to obtain or for misusing consent. This is a reflection of the sensitivity surrounding genetic data.

29. The European Court of Human Rights, in *S and Marper v United Kingdom*, agreed with Baroness Hale there could be little, if anything, more private to the individual than the knowledge of his genetic make-up. It also held that the systematic retention of that material was sufficiently intrusive to disclose an interference with the right to respect for private life. Accordingly, there is a clear privacy interest in protecting genetic data and we consider that data subjects would be likely to experience particular damage or

[2] The English court made precisely this error in *R (Stone) v. South East Coast Health Authority* [2007] UKHRR 137, resulting in publication of a large volume of medical information about a former mental patient.

distress if their or their relatives' genetic data were improperly or insecurely processed. We agree that the Commission should include genetic data in the category of sensitive personal data.

30. Genetic data (such as fingerprints) are used in biometric systems, although "biometric data" is a broader category than "genetic data". Biometrics are physical identifiers of individuals, which are generally used in systems to recognise or authenticate individuals. Examples of biometric systems include fingerprint recognition, hand recognition, vein recognition, gait recognition, face recognition (2d and 3d), iris recognition and voice recognition. Biometric systems operate by creating a mathematical template from the raw biometric information when the individual enrols with the system [see CESG's Biometrics Working Group *Management Summary: Glossary of Biometric Terms* http://www.cesg.gov.uk/policy_technologies/biometrics/ms01.shtml]. The mathematical template renders in mathematical form a certain number of unique identifying points in the biometric (eg certain swirls or angles in a fingerprint). So for example, when an individual's fingerprint is scanned to allow her to log onto a computer, the scanned image is compared to the mathematical template of the enrolled image to see if the identification points match.

31. Some biometric systems retain an image of the raw biometric information which was enrolled (eg to update the template if it is corrupted), but many do not. The UK's Information Commissioner considers encrypted biometric systems which only retain the biometric template to be a "privacy enhancing technology" [DP Guidance Note 29/03/07].

32. In determining whether "biometric data" should be sensitive personal data, a distinction has to be drawn between the raw biometric information (ie the image of the fingerprint or the face or the recording of the voice) and the mathematical template produced from the raw information. Although both the raw biometric information and the mathematical template are personal information, the template by itself is not obviously sensitive personal information. There is not sufficient data in the template to identify, for example, the ethnic origin or race of a person. There is also not sufficient information in the template to recreate the raw data through a process of reverse engineering.

33. However, we consider that the raw biometric information should be sensitive personal data. This case arises from the highly private and personal nature of biological information about the individual and the particular damage or distress which could result if the raw biometric information were improperly or insecurely processed. Where a number of different identification systems or entitlement to a number of services is reliant on biometric authentication, the loss or improper disclosure of raw biometric information could have severe consequences.

The Commission will:

- 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.

34. In 2006, the UK's Information Commissioner twice advocated that custodial sentences should be available for the most serious breaches of data protection by individuals unlawful obtaining, disclosing or procuring personal information. We agree that the Commission should consider the inclusion of such criminal sanctions in the Directive and would support this development.

35. In our experience, the current actions available under the data protection legislation are not well used. The Commission should consider the extension of the right to bring actions to the data protection authority and to civil society groups. However, it is our view that this will not necessarily improve the take-up of the enforcement routes available under domestic data protection legislation. A simpler enforcement mechanism, such as an action for breach of statute, would likely have better results in the United Kingdom. Both courts and advisors are well versed in the principles of breach of statute, which would give courts flexibility in awarding injured parties such damages as are fair and equitable, based on the following non-exhaustive elements:

- the period over which the processing took place;
- the extent of the breach;
- the sensitivity of the information;
- the extent of hurt to the individual, both before and after discovery of the breach;
- any commercial gain to the data processor from the processing;
- whether the breach was intentional/knowing or not;
- how the data controller reacted after initial complaint.

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.**

36. The key purpose of having notification and a public register of data controllers is transparency and openness. It is a basic principle of data protection that the public should know, or should be able to find out, who is carrying out the processing of personal information as well as other details about the processing (such as for what reason it is being carried out). Notification, therefore, serves the interests of individuals in assisting them to understand how personal information is being processed by data controllers.

37. It is neither necessary nor practicable that the notification scheme should require very detailed information about a data controller's processing. The UK Information Commissioner has devised a notification scheme and public register with the aim of

keeping content at a general level, with sufficient detail to give an overall picture of the processing. The Information Commissioner's Office maintains a public register of data controllers. Each entry in the register contains the name and address of the data controller as well as a general description of the processing of personal information undertaken by the data controller. Individuals can consult the register to find out what processing of personal information is being carried out by a particular data controller.

38. The UK Information Commissioner's notification form is available online at https://www.ico.gov.uk/onlinenotification/?page=7.html It includes templated notifications constructed by the Information Commissioner based on the nature of various businesses (eg finance; health; public body; legal; education), which can be amended by the data controller to reflect the type of processing she undertakes. This successfully simplifies the process while still allowing for individuation where required.

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.

39. In general terms, accessing the legal profession and judicial system of another Member State is likely to pose a greater challenge to the individual data subject than to a data controller. We would favour a general rule that jurisdiction and applicable law should be those of the data subject's home State. That could be subject to proportionate exceptions to prevent an inflexible rule causing injustice in particular cases – eg. to cover those situations where the data subject is in reality an entity with greater ability to access legal advice and dispute-resolution machinery than the data controller.

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'**.

40. We agree that the Commission should investigate ways of promoting both Privacy by Design and Security by Design. All too often, technologies are developed and

security measures to protect data are often an after-thought. Security is a process, not a product/solution, and should therefore be considered at the development stage rather than as an add-on. Similarly, measures to protect privacy are often an after-thought, not well integrated into new technologies. In particular, default settings generally do not automatically protect privacy (while then allowing users to choose lower levels of privacy if they wish). All too often, default settings are open and require both technical and operational know-how on the part of the user to increase privacy levels.

41. This is an area where it is imperative that legal policy-makers work together with those who set international technical standards, both in order for data protection principles to inform technical standards and so that those with technical expertise can feed that know-how into the legal process. In this way, privacy and data protection features could form part of the compliance framework for technology sectors, and legal concepts (such as "data controller") could be revised to take into account the way technologies actually work.

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.

42. We would support self-regulatory initiatives provided these are **additional** to and in no sense **in substitution for** effective mechanisms for providing guidance to those processing personal data and for enforcing the rights of data subjects.

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, e.g., 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 co-operation in criminal matters in specific instruments**, with the new general legal data protection framework.

43. It is important in any society governed by the rule of law that there are no "no go areas" for the privacy rights of data subjects. While there may be a case for carefully tailored exceptions for certain operations where secrecy of State activity from the data subject is of the essence, those should go no further than absolutely necessary. For example, where an investigation has been concluded, or an individual charged with an offence, it is hard to see any compelling justification for continuing to deny subject access rights.

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.

44. We agree that the current procedures for international transfers should be improved. The insistence of an appropriate level of protection for the rights and freedoms of data subjects in all exports of personal data to non-EEA countries is an important tool to prevent wholesale avoidance of the protections contained in the Directive. That insistence has also had significant beneficial effects in bringing a higher level of information protection to non-EEA countries: the uptake of Safe Harbor rules by a sizeable number of US companies (well over 1500) is a stand-out example.

45. However, it must be acknowledged that the current system is cumbersome, complex and costly and that it puts significant strain on multi-national organisations. Globalisation and emerging technologies, such as cloud computing, stretch the model contract framework almost to breaking point.

46. We agree that one way forward may be for the Directive to recognise in a more formal way the use of group-wide codes of conduct as an acceptable mechanism to deliver adequacy. These Binding Corporate Rules ("**BCR**") allow companies to work with national supervisory authorities to adopt binding internal codes which can be approved under Art 26(2) if they deliver guarantees of compliance and rights of redress. This is a very useful way in which businesses can work closely with data protection authorities to secure adequate safeguards for the transfer of information within a group of companies.

47. The UK's Information Commissioner has produced a checklist for BCR approval (which also found favour with the Article 29 Working Party, as the IC's approach was adopted in the Working Party's Model Checklist Application for Approval of BCR

[05/EN WP 108]). The Working Party has also produced an application form for BCR [07/EN WP 133]. We endorse this approach.

48. BCRs can work in conjunction with contractual solutions, with an initial transfer being made under the BCR and subsequent onward transfers being covered by separate contractual solutions.

49. However, these solutions are not fit for new technological advances, such as cloud computing. Clients in a cloud structure do not purchase servers, software, data-centre space or network equipment, but instead buy those resources as a fully outsourced service in "the cloud". Even the service providers to the cloud may not know which physical processors in which countries are processing information at any one time. The only practical way in which data protection can be applied to technology such as cloud computing is for international standards for data protection and privacy to be adopted, which would operate as a global indication of adequacy of protection.

50. We suggest that the Commission should build on the success already achieved in November 2009 at the 31st International Conference of Data Protection and Privacy Commissioners, with the adoption of the Resolution on International Standards of Privacy ("**the Madrid Resolution**"). The Madrid Resolution is the first step towards a binding international set of standards for the protection of personal information. Should such binding standards be agreed, every country adhering to the standards would be considered to provide adequate protection for personal data. The wide-scale adoption of a single set of international standards would significantly facilitate safe cross-border processing.

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.

51. As mentioned above, we support the adoption of a single set of International Standards of Privacy – this designation properly emphasised that the protection of privacy is the central animating principle of data protection.

52. It is imperative that technical standards and legal rules "talk to" each other rather than past each other. Given the enormous impact that technology is having and will continue to have in the area of data processing, we would urge the Commission to ensure that people with sufficient technical expertise are available to consult on any reforms to the Directive. It is only through the proper collaboration of legal policy makers and those with technical know-how that data protection rules can evolve to confront the challenges of the e-environment.

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.**

53. The Commission should consider whether there is a case for conferring certain regulatory and enforcement powers as against data controllers directly on a body at EU level. It is a moot point whether the authorities of individual Member States are able to act in concert to the degree necessary to ensure effective enforcement of the legislation against the largest data controllers - Google, Microsoft, and so on -- who operate in many Member States. This is the approach taken in other areas of EU regulation, notably competition law. One possibility would be to confer powers on a strengthened European Data Protection Supervisor. If powers are conferred on a central authority at EU level however, those powers should be limited to cross-border situations, and its decisions must be amenable to judicial supervision at that level.

Estelle Dehon
Gordon Nardell QC.

Approved by the
Law Reform Committee,
European Committee,
of the Bar Council of England and Wales

January 2011