

Microsoft Response to the Commission Communication: A comprehensive approach on personal data protection in the European Union

15 January 2011

I. Introduction

Microsoft's success depends on users having confidence in our ability to responsibly manage and protect their data. To that end, we have worked hard to ensure that all of the company's products, services, processes and systems incorporate measures designed to help protect user privacy. We also work closely with regulators, industry and civil society organisations to develop responsible business practices and strengthen national and international legal frameworks for data protection.

Given our commitment to data protection, Microsoft welcomes the opportunity to participate in this important consultation on "*a comprehensive approach on personal data protection in the European Union*". For over a decade, the EU's Directive 95/46/EC has provided strong protections for the personal data of Europe's citizens. In recent years, however, it has become increasingly evident that dramatic and rapid technological change – the hallmark of the last decade – is placing parts of the Directive and its current implementation in Member State law under stress. The explosive growth of the Internet economy, cloud computing, the proliferation of computers and handheld mobile devices, and the expansion of e-commerce, e-government, e-health and other web-based services have brought us tremendous social and economic benefits. At the same time, these technologies have fundamentally redefined how, where, and by whom data is collected, transmitted and used – testing how to implement fundamental concepts underpinning EU data protection law, such as notice and consent, jurisdiction, and geographic limitations on data flows.

There is no going back. Today's generation will never know life before the Internet. Instead, the use of devices that fit in our pockets to access data from wherever we happen to be has become an integral and expected part of our daily lives. We search the web, read newspapers and purchase music from our smart phones. European social network users access and update their profiles when holidaying in the U.S. and Asia, and business executives access their e-mail and download documents from points across the globe. Commuters rely on GPS to guide them to their destinations, while transport drivers with handheld computers travel around the EU, rerouting deliveries in response to customer needs. This technological transformation will only accelerate in the coming decade as the number of Internet users expands, the speed and capacity of networks increase, the range of smart devices grows and Internet-enabled services become more prevalent.

The “cloud” has been a centrepiece of this technological transformation. Once used primarily for consumer facing services such as e-mail, cloud users (including governments and enterprises) today are storing and sharing unprecedented amounts of information online, leading to a fundamental expansion in the magnitude and types of data being collected and used. This data may be stored on servers in multiple countries, belong to customers in jurisdictions across the world, and move routinely across national and regional borders.

Cloud solutions are poised to grow dramatically in the coming years, offering great promise for Europe, including its citizens, governments and industry. Among other benefits, analysts estimate that cloud computing could create, on average, a million new jobs and several hundred thousand new small and medium-sized companies (SMEs) in Europe.¹ Cloud computing also has the potential to drive down the cost of ICT for the public and private sectors, and to transform the relationship between European citizens and their governments, leading to more transparent and efficient interactions. But these and many other web-enabled benefits will only be realised if users have confidence that their data is safe in the cloud. The challenge that we in the ICT sector thus face – and must work together with regulators and other stakeholders to answer – is how to best protect users’ privacy while enabling innovation and facilitating the productivity and cost-efficiency offered by new computing paradigms like cloud computing.

To address this challenge, the next generation of privacy regulation in the EU needs to achieve two ends: it must provide robust protections to users, while at the same time enabling European companies not only to select from a wide range of competitive online services offerings, but also to compete by offering their own services on a European as well as a global basis. Next generation privacy regulation must also be “future-proof” to the greatest extent possible, in order to withstand the rapid pace of technological change and protect personal data not only on the day of adoption, but 5, 10 and even 15 years later.

To achieve these ends, we believe that each provision of any proposed data protection legislation should be tested against certain fundamental criteria, among them:

- Certainty. The patchwork of local, national and regional legal and regulatory frameworks governing data protection has become increasingly difficult for companies of all sizes to comply with as ever-larger volumes of data move across different geographic boundaries. This patchwork must be replaced by a true digital single market for personal data – ideally globally, and certainly in Europe. Any reform of the EU framework must introduce greater harmonisation across the Community’s 27 Member States. At the same time, greater clarity is needed – including with regard to what law or laws apply to the processing of data – so that those handling data have a clearer

¹ F. Etro, “The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe”, Review of Business and Economics, 2009/2, pp. 191, 192.

understanding of their obligations. This will ensure a consistently high level of protection for European citizens, and much-needed legal certainty for data controllers.

- **Flexibility.** We believe that a greater focus on achieving substantive outcomes – and a reduced emphasis on applying prescriptive rules and complying with formalities – will render data protection regulation more resilient and more durable. Regulations crafted in this way give organisations the flexibility to adapt their policies and practices to meet changing scenarios, while still subjecting them to the obligation to provide strong privacy protections. This approach tracks the much-discussed notion of accountability, and we are pleased that the Commission is thinking about how it can better integrate accountability-based measures into the EU’s regulatory regime.
- **Simplified data flows.** Today, data is no longer constrained within geographic silos to the extent that it was when the EU first adopted Directive 95/46. Instead, personal data regularly crosses national and international borders. It is important to acknowledge this trend and improve existing mechanisms for international data transfer to ensure that they continue to protect users while facilitating the data flows necessary to enable more efficient, more reliable, and more secure delivery of online services to Europe’s consumers at lower prices.
- **Technology neutrality.** There is no question that technology will continue to change – and change quickly. Legislative preferences for particular services, solutions or mechanisms to protect data will quickly be superseded by new technologies. Today, for example, there is significant debate over how best to secure effective user consents by means of Internet browser settings. Preferences for one approach over another can chill innovation, deterring providers from developing alternative approaches to protect data.

These are unquestionably challenging times – but also exciting ones – for those concerned with the protection of data. Microsoft welcomes the opportunity to work with the Commission and other stakeholders to help improve Europe’s solid regulatory foundation so that it is better suited to today’s more complex privacy environment. Our comments on the specific issues raised in the Commission’s Communication follow.

II. Strengthening Individuals’ Rights (Section 2.1)

A. Ensuring appropriate protection for individuals in all circumstances (Section 2.1.1)

- **To ensure the consistent protection of data, national regulators must take a more uniform view of the concept of personal data. The challenge for the Commission will lie in introducing greater uniformity while still preserving enough flexibility to permit the regime to accommodate new types of data that emerge in the future.**

- **The current definition of “personal data” in Directive 95/46 has the benefit of being broad enough to encompass future data types. If the Commission chooses to retain this definition, however, the Commission should provide clear guidance to ensure that Member States more uniformly interpret and apply it along with mechanisms to enforce that guidance.**
- **Expanding the scope of the data protection regime to apply to other forms of data, such as certain types of location data, is unnecessary. This data is already covered where it relates to an identifiable individual. We likewise see no need to expand the current categories of sensitive data at the present time.**
- **More broadly, to help ensure appropriate protection for individuals in all circumstances, we encourage the Commission to consider a “use and obligations” model, where the protections afforded depend more on the context in which data is processed than on the type of data involved.**

The scope of Directive 95/46, and the issue of what data qualifies as “personal data,” are among the most fundamental issues in the EU reform process. On the one hand, it is clear that greater uniformity in how Member States interpret the concept of personal data is needed. Frequently, there is a lack of consensus among regulators over whether certain data should be deemed – the result in part of divergent Member State implementations of the term “personal data” in the Directive – meaning that data that qualifies as personal data in one country may not qualify as such in another; there are likewise significant national divergences in terms of the specific types of data that are deemed to be sensitive, particularly with regard to health-related data (e.g., some Member States specifically include biometrics or genetic data while others do not). On the other hand, introducing rules that more precisely delineate what data is and is not personal (or sensitive) may undermine the regime’s flexibility, limiting its ability to accommodate new types of data.

The current formulation for “personal data” in Directive 95/46 – which captures any sort of information, regardless of form or content, where that information relates to an identified or identifiable natural person – has the benefit of adaptability. If the Commission retains this approach, however, we strongly encourage it to take steps to clarify its interpretation and scope. Specifically, we recommend that the Commission:

- Provide clear guidance in terms of what falls within the definition and what does not, including where the line is to be drawn in terms of when data relates to an individual and when it does not (as the Article 29 Working Party attempted to do in its Opinion 4/2007 on the concept of personal data). Currently, for example, some Member States take an overly broad approach that sweeps virtually all data within the definition. Clearer guidance would help to promote uniformity, and would offer data controllers greater legal certainty; and
- Adopt measures to ensure that there is consistency in the application of this guidance at the national level. One option (which we describe more fully below, in

our response to Section 2.2.1) would be for the Commission to restructure the Article 31 Committee so that it has competence to more closely oversee implementations of the revised Directive, including rules on what constitutes personal data.

We see no need to expand the scope of the data protection regime to apply to other forms of non-personal data, such as certain types of location data. Under the current, broad test, location data that is linked to an identifiable person is already covered. In contrast, location data that is not related to an identifiable person (e.g., that relates to a wireless router, such as SSID information (the name of a wireless local area network) or MAC address (a globally unique identifier for wireless network hardware)) raises fewer privacy concerns and does not merit regulation as personal data *per se* under the EU data protection framework. Deeming this data “personal” would only serve to create obstacles in providing the geographic location services demanded by consumers without enhancing their privacy.

We likewise see no need to expand the current categories of sensitive data at the present time. However, we do encourage the Commission to reduce divergences with respect to the sensitive data rules by making the list included in the Directive exhaustive, and thereby limiting the ability of Member States to deviate from it. Some Member States extend the Directive’s restrictions on processing sensitive data to other categories of data, such as genetic data and biometric data – creating compliance challenges and an uneven patchwork of rules across the EU.

More generally, to help ensure that individuals are appropriately protected within the EU’s data protection framework in all circumstances, we encourage the Commission to consider a “use and obligations” model, where the protections afforded depend less on the type of data involved (i.e., personal/sensitive) and more on the context in which that data is processed. For example, an individual’s name appearing on a company intranet page listing employees would be afforded less robust privacy protections than the same name appearing on a “black list” related to credit ratings. (Of course, certain sensitive personal data, by its very nature, would be subject to high levels of protection in all contexts.) This would differ from the current EU regime, where unless data is sensitive it enjoys no special protection (beyond that afforded to any other personal data), no matter the context in which the data is used. We do note that some Member States have adopted rules that echo this approach; in Austria, for example, coded data is subject to fewer protections when processed by an entity that does not have the key to the code.² The proposed approach would also track Article 17 of Directive 95/46, which contemplates that security measures for personal data should be context based, that is, “appropriate to the risk presented by the processing”. We set out our recommendations regarding this approach further in Section II.D (Ensuring informed and free consent) below.

² Datenschutzgesetz 2000 – DSG 2000, Bundesgesetzblatt, 17 August 1999, as amended, Article 2, §4(1). Available at www.dsk.gv.at/DocView.axd?CobId=41936

B. Increasing transparency for data subjects (Section 2.1.2)

- **Microsoft supports the Commission’s efforts to enhance transparency by building on Articles 10 and 11 of Directive 95/46. We agree that data subjects can exercise choice only when they are clearly and fully informed of how their data is collected, used and shared. Given the many different contexts in which disclosures are furnished, data controllers should be given latitude to determine what method of notice and formulation of language will be most appropriate.**
- **Microsoft also supports the introduction of a generally-applicable breach notice regime. To avoid the issuance of immaterial notices that consumers ultimately come to ignore, the obligation to notify a breach should be triggered by a significant risk of serious harm. Notification should not be required, in contrast, where the potential harm is nominal, such as where information is encrypted or otherwise unintelligible to those not authorised to access it.**
- **While broad guidance regarding what should be included in a notice (consistent with requirements under the amended e-Privacy Directive) would be welcomed, the method of notice should remain flexible and be left to the service provider.**
- **In implementing both the transparency obligation and data breach rules, the ability of Member States to introduce additional requirements should be restricted. Otherwise data controllers will find themselves once again facing a web of different national requirements across the EU.**

One of the central tenets of Microsoft’s own privacy principles is that users must have choice over how we use and disclose their personal information. Our customers can only exercise this choice in a meaningful way if they are clearly informed about how we intend to process their data. For this reason, we have been at the forefront of efforts to promote transparency in the online space, including being one of the first companies to deploy so-called “layered notices” to better inform users regarding our data handling practices. Our own experience has demonstrated that providing notice in ways that are clear and easily accessible has helped to promote the uptake of our technologies and services, and encourages Internet usage more broadly.

We thus support the Commission’s efforts to enhance transparency by calling for the provision of additional information to data subjects, building on the rules established in Articles 10 and 11 of Directive 95/46. Among other things, EU notice rules could require, for example, that data controllers disclose information to users about their rights to access, rectify, or delete their data, where such disclosures are not already required by national-level laws – while leaving it to individual data controllers to determine the most appropriate formulation of the relevant language.

While we support an obligation to provide clear and thorough notices, we do not believe that legislation should dictate the method by which users are informed. Specific methods for

providing information can quickly become obsolete, and may ultimately lead to reduced privacy protections by eliminating incentives to develop better methods of communicating with data subjects. Likewise, because the effectiveness of notices can be undermined by providing too much information just as it can be by providing too little, data controllers should have reasonable discretion about what information to disclose. For example, there should not be an obligation to disclose where and by which employees or subcontractors data is being processed – disclosures that would unnecessarily restrict a service provider’s flexibility to change where and through whom it processes data.

Consistent with our view that information is essential to effectively exercise choice, we also support a generally-applicable breach notification obligation. A general obligation on data controllers to provide notification regarding serious data breaches will enable users to better protect themselves; such an obligation will also drive a higher standard of data security across industry. While a general regime could build off the rules recently adopted in the 2009 amendments to the e-Privacy Directive (Directive 2009/136/EC), some modifications to the e-Privacy Directive rules will likely be required to reflect the fact that the instant regime will apply to all sectors. For example, it may be appropriate to require notification in more limited situations in order to ensure that data subjects do not suffer from “notification fatigue” and ultimately ignore notices.

Specifically, to ensure that notices remain effective, data controllers should be required to notify data subjects and/or regulators of a breach only when there is a significant risk of serious harm to the data subject. (Germany’s breach regime, which is premised on the threat of a serious harm, provides one potential model in this regard.³) Criteria to be considered in making this assessment could include the type of data involved and its sensitivity; the nature of the breach (i.e., has the data been stolen? or merely damaged or altered?); and what harm is threatened by the breach (consistent with the regime established under the e-Privacy Directive, harms meriting notification could include risk of identity theft, fraud or physical harm).

In contrast, notification should not be required where the potential harm is nominal, such as where information is encrypted or otherwise unintelligible to any person who is not authorised to access it (following the approach adopted in Article 4(3) of the e-Privacy Directive). Requiring notifications only where serious harm is threatened reduces the likelihood that data controllers issue immaterial notices that may lead, over time, to consumers ignoring them.

Guidance on the content of notices would be useful. The parameters established in Article 4(3) of the e-Privacy Directive relating to the content of notices strike a good balance between providing notice recipients with necessary information while not overwhelming them: the notice should describe the nature of the breach, provide a contact point where individuals

³ Federal Data Protection Act (BDSG), in the version promulgated on 14 January 2003 (Federal Law Gazette I, p. 66), last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, p. 2814), in force from 1 September 2009, Part IV, Section 42a., available at http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?_blob=publicationFile.

can acquire additional information, and recommend mitigating measures to the possible adverse effects of the breach.

We do not believe that legislation should dictate the method of notice. Instead, the method should remain flexible and be left to the choice of the service provider. This will permit data controllers to communicate with their customers in the way that is most sensible, efficient and effective given the circumstances. Moreover, where individualised notice to data subjects would be impractical or require a disproportionate effort (for example, due to the number of individuals affected or if the data controller does not possess the contact information for the affected individuals), then it should be permissible to use other methods of notification.

In implementing these obligations – transparency and breach notice – it is essential that Member States are limited in their ability to introduce additional requirements on top of the obligations established in any EU instrument. Divergences from market to market create significant compliance burdens for pan-EU providers, while adding little benefit in terms of enhanced data protection. We thus would have significant concerns with the introduction of a provision along the lines of Article 4(4) of the e-Privacy Directive, which permits Member States to adopt guidelines regarding the circumstances in which providers are required to notify breaches, format of such notification and the manner in which notification is to be made. Instead, any breach notice regime should include a provision making clear that the Commission, in close consultation with national authorities and other stakeholders, will establish any necessary technical implementing measures concerning the circumstances, format and procedures applicable to information and notification requirements.

C. Enhancing control over one's own data (Section 2.1.3)

- **Microsoft believes that the ability to retrieve data is an essential element of a user's control over that data. We thus support the introduction of rules designed to encourage online service providers to give users easy and efficient ways to retrieve their own data.**
- **In crafting such rules, the Commission should clearly distinguish between *user* data and data generated in the operation of the service; should extend the obligation only to data retained by the service provider; and should recognise that because of technical realities, retrieved data cannot necessarily be used "as is" in other services.**
- **Alternatively (or in addition), the Commission should also consider obligating online service providers to disclose to users, in a simple and easy-to-understand manner, what data they can export. This will enable users to better comprehend and compare the portability policies and practices of service providers.**
- **Clarification and further harmonisation of the existing right to erase data (the "right to be forgotten") may also be warranted. To be workable in practice, the obligation**

to erase data should again be limited to user data retained by the service provider; apply only to that data which is under the service provider's control and is reasonably accessible in the ordinary course of business; and be satisfied by the anonymisation (rather than deletion) of data. Service providers should also be permitted to retain data for a limited period in order to re-enable customers where they so desire.

Microsoft understands that the user is the owner of the data he or she inputs, whether in software on the desktop or a service in the cloud. An essential element of a user's control over that data is the ability to retrieve that data in a simple and cost-efficient way. As we develop our cloud services, Microsoft strives to build capabilities into those services to give the user that control. For example, Windows Live is a collection of cloud based services that includes an online photo album where users can upload pictures and store them on a cloud-based storage system. Windows Live has built-in capabilities through a readily-accessed menu option for users to retrieve all of their pictures quickly and easily.

We are similarly focused on data portability in the context of our cloud computing services. Our customers have been clear that they want the ability to move data among heterogeneous cloud services without incurring significant switching costs. Microsoft recognised the importance of data portability as part of our [Interoperability Elements of Cloud Platforms](#) published in 2010. We facilitate customers' ability to move data in and out of the cloud through various technologies; SQL Azure, Windows Azure Storage and Live Contacts API, for example, make it possible for customers to move their data into and out of these services.⁴

We support the EU's efforts to reinforce market demand by introducing rules aimed at requiring online services providers to give users easy and efficient ways to retrieve their own data, where this is technically and commercially reasonable. To complement this right (or perhaps as an alternative to it), the Commission should also consider obligating online service providers to disclose to users, in a simple and easy-to-understand manner, what data they can retrieve and how – for example, what formats are available for export and what (if any) costs the provider charges for export. This would at least enable users to better compare providers' data portability policies and practices and make informed choices.

To be workable, the right must reflect technical realities and an understanding of how the Internet and online services operate. To that end, we encourage the Commission to recognise that compliance should be required only when it is technically and commercially reasonable. We also encourage the Commission to be guided by the following when defining the right of data portability:

- First, the right must draw clear distinctions between a user's own data – i.e. data that the user inputs directly (and, as described below, is retained by the service provider), such as e-mails, names of contacts, passwords or photos – and data

⁴ For further information on how Microsoft enables data portability in the cloud, see <http://cloudinteropelements.cloudapp.net/data-portability.aspx>

generated in the operation of the service (for example error messages or uptime statistics). While users should be able to retrieve the former, there should be no obligation on service providers to make the latter retrievable. In addition, application programs and games that run on the services are not user data and should not be subject to this requirement. (Clearly delineating the scope of user data – an exercise that should be undertaken in close consultation with industry – will also help to avoid the problem of Member States taking different approaches to what can and cannot be exported.)

- Second, the right should be limited to user data that is retained by the service provider. This recognises the technical reality that the user sometimes creates data that service providers do not retain, such as bits lost during compression, bits or formatting lost during file format translation, etc.
- It is also important to recognise that the right to retrieve data does not necessarily mean that such data can be used “as is” in other services. There are several means to achieve portability, including industry standard formats, documented non-standard formats, import/export functions and APIs permitting others to connect to the data directly – all of which rely on a data format to export and transfer the data. While there are very good formats to exchange many types of data in the industry and many systems that can share information effectively, few services store information in the formats typically used for data exchange, so the export process itself has potential for some loss of information, including data, layout or formatting. This can occur in the export to a transfer format, conversion between system formats, as a result of different features between one system and the next, or even as a result of different approaches in implementing the same format. Given this, achieving data portability can be technically challenging, and the degree of success depends upon work of all of the service providers involved in the export, translation and import of data.
- Ultimately, the right should recognise that the service provider is responsible for the choice of formats, and should encourage service providers to balance the numerous technical issues involved in making this choice reasonably in an effort to return data to the user in a usable form. For example, in general, the richer the data format, the more it is likely to be associated with the specific functions of a service or application (such as a documented email storage format like PST) and hence is directly consumable by a smaller number of services or applications. In contrast, the more widely a format can be used (such as the MIME email standard format), the less it can fully reproduce things like layout, format and images in the way the user first entered them. The choice involves technical and commercial trade-offs that the technology provider is best situated to assess.

We also support the Commission’s proposal to better harmonise the rules relating to individuals’ existing rights to access, rectify and erase their data. Currently, Member States take divergent approaches to the implementation of these rights; greater certainty would benefit

data subjects and data controllers alike. As part of this effort, clarification of the right of erasure (the so-called “right to be forgotten”) may also be warranted. Indeed, Microsoft is already working hard to develop tools that allow users to limit the data trail that they leave behind. For example, InPrivate Browsing in Internet Explorer 8 helps to prevent the Internet user's browsing history, temporary Internet files, form data, cookies, and usernames and passwords from being retained by the browser, leaving no evidence of the user's browsing or search history. While the browser is in use to surf the Internet, IE8 stores some information, such as cookies and temporary Internet files, so that the web pages visited will work correctly – but at the end of the InPrivate Browsing session, this information is discarded. (IE8 will also launch a browser session that won't record any information, including searches or webpage visits.) In our search business Bing, our current practice is that as soon as Microsoft receives a Bing search query we take steps to de-identify the data by separating it from account information that could identify the person who performed the search. Then, at 18 months, we take the additional step of deleting the IP address, the de-identified cookie ID and any other cross-session IDs associated with the query.

In clarifying the concept of a right to be forgotten, it is important to recall that in today's online ecosystem, where users participate in a wide range of social networks and use a broad range of technologies, and where digital data is often replicated on a number of different servers and systems (some of which are not under the control of the service provider), it may not be commercially reasonable or even possible to “remove all tracks.” In some situations, removing all tracks may affect other users' rights; in other scenarios, it will take an unreasonable effort. To be workable, implementation of the right to be forgotten should require data controllers to delete only that data which is the user's own data (as described above); is under the control of the service provider; and reasonably accessible in the ordinary course of business. Data controllers also should be permitted to comply with this right through an effective process of anonymisation or “de-identification” of data. Finally, to facilitate the efficient “re-enabling” of services where a user so desires (such as when a user deletes an account by mistake), data controllers should be permitted to keep certain essential data for a limited period of time following a request for deletion.

D. Ensuring informed and free consent (Section 2.1.5)

- **In light of the dramatic growth in data flows in recent years, existing notice and consent requirements are no longer sufficient to adequately protect rights in personal data. Microsoft encourages the Commission to consider adopting a “use and obligations” model, where the uses to which any data are put – rather than the circumstances under which the data is collected – serves as the primary driver of obligations to protect data.**
- **In circumstances where individual consent may still be necessary, the Commission and national regulators should focus on the ends, not the means, in obtaining consent, especially on-line. EU rules should recognise the validity of a range of mechanisms for**

consent, including an informed opt-out, rather than preferring one mechanism over another; all such mechanisms should be required to enable meaningful consent in the particular context in which they are deployed.

Where it is appropriate or necessary under the current EU data protection framework for a data controller to acquire an individual's consent to process personal data, such consent must be a "freely given specific and informed indication" of the individual's agreement to such processing. However, as the Commission recognises in its Communication, Member States have different rules regarding how individuals may signify consent, with some recognising only express and sometimes only written, consents and some others appearing to accept implicit consents. This inconsistency and lack of clarity undermines Directive 95/46's data protection framework.

While the Commission's intention to clarify the conditions for obtaining valid consents would be welcomed, the present consultation affords an opportunity to update the law to ensure that individuals can effectively exercise their right to protect their personal data in the context of modern processing practices. With the enormous growth in data flows in recent years, accompanied by new technologies and business models that use information in unanticipated ways, notice and consent mechanisms can be insufficient to adequately protect rights in personal data. In today's world, it is increasingly unrealistic to expect individuals to review every privacy notice or to make informed choices given the quantity of information with which they are provided, and unreasonable to continue to ask individuals to assume primary responsibility for policing use of their data. And yet the current framework, based on notice and consent, imposes exactly this burden.

Microsoft encourages the Commission to consider moving towards a "use and obligations" model that places greater emphasis on the uses to which data are put – rather than the circumstances under which the data is collected – to determine obligations in relation to processing the data. This model does not replace the need for appropriate individual participation through notice and consent policies, but rather addresses the current over-reliance on consumers to monitor how their personal data is being processed. Data controllers would still be required to provide individuals with appropriate notice about how they collect and process their data, but the substantive obligations would largely depend on how controllers use the data and there would be reduced reliance upon individual consents. Obligations would vary depending on the level of risk associated with different uses, such as processing to establish and maintain a contractual relationship with an individual, for internal business purposes, or when complying with legal requirements. This improves on the notice and consent regime by holding each entity that processes personal data more directly accountable for regulating its processing while still ensuring that individuals can participate at an appropriate level. This approach is in line with a broader focus on "accountability", which we comment on in greater detail in Section III.D (Enhancing data controllers' responsibility).

While we believe that a "use and obligations" model is better suited to present and future data processing practices, Microsoft recognises that this would signify a departure from existing EU rules. If the Commission considers this approach to be unworkable, and to the

extent that circumstances remain where it may still be necessary to obtain individual consent, we would encourage the Commission and national regulators to focus on the ends, not the means, in obtaining consent, especially on-line. An overly rigid approach to obtaining consent on-line focused on requiring the use of particular mechanisms (e.g., opt-in) rather than on ensuring meaningful consent offers little gain in terms of privacy protection while imposing significant costs; such an approach may also quickly become obsolete given the rapid pace of technological change.

There are currently a wide range of mechanisms that enable users to control and consent to collection and use of their information, and some of the more robust opt-out mechanisms provide stronger protection for consumer privacy (with fewer disruptions for Internet users) than weaker opt-in mechanisms. Indeed, given that modern websites increasingly pull content from multiple sources, requiring users to provide separate opt-in consents in relation to every site that is the source of content would result in users receiving a significant number of opt-in requests every time they go online – a situation which often leads to users opting-in as a matter of routine, even when their privacy would be better served by their opting out. We thus believe that EU rules should recognise the validity of a range of mechanisms for consent, including an informed opt-out, rather than preferring one mechanism over another – but should require that all such mechanisms enable meaningful consent in the particular context in which they are deployed.

We also note that preferences for particular mechanisms for obtaining consent can chill innovation in privacy protection and deter technology providers from developing more privacy protecting solutions. For example, our next generation Internet browser, IE9, will include significant new innovation – specifically, a technology that will enable users, through the use of “Tracking Protection Lists” (“TPLs”), to control what levels of privacy protection they want when browsing the web. TPLs, which are simply files that can be uploaded to a website and made available to others via a link, can be created by anyone on the web; they may include “do not call (or visit)” lists that will block third-party content, including cookies and similar files, from any site that is listed on the TPL, unless a user visits the site directly by clicking on a link or typing its web address. By limiting calls to these websites, IE9 will restrict the information these third party sites can collect about web users. The impetus to develop innovations such as these will be diminished if EU regulations prefer one mechanism for control over another.

Finally, regarding consent, if the status quo is to be maintained, we also encourage the Commission to recognise that where processing of personal data falls within a user’s reasonable expectations given the context of the processing, then notice and consent become less necessary. A number of national Data Protection Authorities (“DPAs”) already embrace this principle, concluding that where secondary processing by an organisation is within the user’s reasonable expectations, further notice is not required.

E. Making remedies and sanctions more effective (Section 2.1.7)

- **The current national provisions regarding sanctions for violating data protection rules vary significantly and enforcement is inconsistent. Reforms may be appropriate to ensure that DPAs have a clear and consistent regime to apply and the power to impose meaningful sanctions for serious violations.**

Effective regulatory regimes require clear and meaningful sanctions for violations of their rules. However, Directive 95/46 only requires Member States to adopt “suitable measures” to ensure the full implementation of the Directive and to lay down “sanctions to be imposed” in case of infringement of its provisions. No further guidance is given or requirements stipulated. The result has been that national provisions regarding sanctions, and efforts to enforce those sanctions, vary significantly across Europe. The approach of different national DPAs ranges from strategic, risk-based approaches that seek to deter non-compliance and minimise data protection risk (and maximise often limited regulatory resources) by targeting those violations that create a real risk of serious harm, to more bureaucratic approaches where compliance with the law is sought as an end in itself.

We thus agree with the Commission that considering the effectiveness of the existing sanctions regime may be warranted. Ultimately, it may be necessary for the Commission to undertake reforms in this area in order to foster a culture of respect for data protection – specifically by ensuring that DPAs have a clear and consistent regime to apply, and have the power to impose serious sanctions for flagrant or repeated violations that threaten real harm to the individuals affected.

The UK regime provides a good example of such sanctions: following recent changes to the Data Protection Act 1998 (the “UK DPA”), the UK Information Commissioner now has the power to impose significant fines – up to a maximum of £500,000 – where the Information Commissioner is satisfied that a contravention is serious and is likely to cause substantial damage or substantial distress, and that the data controller either (i) deliberately contravened the UK DPA or (ii) knew or ought to have known that there was a risk the contravention would occur, and that it would be likely to cause substantial damage or distress, but still failed to take reasonable steps to prevent it from happening. Such increased powers provide a meaningful deterrent and are likely to lead to improved privacy protection for individuals; at the same time, the sanctions are properly limited to truly bad actors.

III. Enhancing the internal market dimension (Section 2.2)

A. Increasing legal certainty and providing a level playing field for data controllers (Section 2.2.1)

- **The advent of new technologies has highlighted divergences among national implementations and interpretations of Directive 95/46. These divergences mean that the rules regulating personal data vary from country to country in important respects and that personal data does not enjoy the same protections in every EU market.**

- **One way to achieve greater harmonisation and a true digital single market for personal data would be to replace the Directive with a directly-applicable regulation. If this is politically unachievable, the Commission could instead empower the Article 31 Committee to monitor and report on divergent national obligations, which could then be remedied or mitigated. In addition, the revised Directive should enable mutual recognition wherever possible.**

The existence of significant divergences among national data protection regimes is well recognised, and has been documented by the Commission as well as in a number of third party studies. These divergences have been starkly highlighted by the advent of modern computing technologies. Online service providers now routinely handle the data of citizens from multiple Member States, and often process personal data in multiple markets in and outside the EU. In doing so, they often find themselves subject to different – and sometimes conflicting – national rules governing what constitutes personal data, what data is sensitive, who is a processor and who is a controller, what principles govern the processing of data, what constitutes consent and what security measures to apply.

Ultimately, diverging national regulatory regimes have undermined the objective of creating a single European market relating to personal data. Divergent regimes also effectively mean that personal data may not enjoy the same robust protections in every Member State.

The EU's ability to achieve a digital single market where data flows freely depends on greater harmonisation of the Union's data governance rules. We thus welcome the Commission's commitment to examine the means to achieve further harmonisation of data protection rules at the EU level. One potential way to achieve this would be for any new data protection instrument to take the form of a directly applicable regulation, rather than a directive, as the Commission initially considered in the early 1990s before adopting Directive 95/46. Alternatively, the Commission could propose a directive premised on the concept of full harmonisation, where the ability of Member States to adopt divergent national laws is limited.

If these approaches are untenable for reasons of competence or subsidiarity, another – albeit potentially less effective – option would be to task a Committee of Member States and Commission representatives to regularly and thoroughly monitor the Directive's implementation and application at national level. The Article 31 Committee established in Directive 95/46 could be used for this purpose (at present, the Committee only has specific authority to act on certain matters relating to international transfers). The Committee – which, unlike the Article 29 Working Party, includes as participating members both representatives of the Commission and the Member States – should among other things be obligated to report where national implementations are inconsistent or obligations are divergent; such findings should be made publicly available, and should be followed by appropriate measures by the Commission, including enforcement actions where necessary.

Finally, a revised Directive should enable mutual recognition between Member States wherever possible. This would be particularly relevant in resolving issues arising from different national-level registration obligations, and in streamlining the binding corporate rules process to

facilitate flows of data to recipients outside the EEA. In parallel, the Commission should modify the existing applicable law regime so that data controllers no longer find themselves subject to multiple Member State laws; we describe our views in this regard in greater detail in Section III.C (Clarifying the rules on applicable law and Member State's responsibility).

B. Reducing administrative burden (Section 2.2.2)

- **Current requirements to notify data processing activities in every Member State where processing occurs are extremely burdensome and do little to enhance data protection. We encourage the Commission to replace existing notification requirements with a single registration form and system of mutual recognition across the EU.**

We strongly support the Commission's efforts to simplify and harmonise DPA notification requirements and welcome the idea of a single registration form. Because Member States have widely varying requirements for registration, the obligation that a company register in every Member State in which they function as a data controller becomes extremely burdensome and costly – without offering a corresponding benefit in terms of enhanced protection for individuals' personal data. A single registration form would reduce the burden of notification considerably. This should be part of a mutual recognition system whereby notification using the single form in one Member State, perhaps performed by the company's primary establishment for processing personal data, would constitute notice in all Member States. As part of this streamlining initiative, we encourage the Commission to narrow the types of information that data controllers must provide when notifying, particularly given that they already are required to make broad informational disclosures to individuals about what data they collect and how they process it (and individuals generally do not look to DPA registrations for this information).

C. Clarifying the rules on applicable law and Member States' responsibility (Section 2.2.3)

- **The rules in Directive 95/46 governing the application of national data protection laws are vague and confusing, and compound the problems arising from divergent Member State regimes.**
- **The Directive's applicable law provisions need to be revised, not only to ensure greater legal certainty for users and data controllers, but also to better cope with new technologies and increased globalisation of services.**
- **Microsoft agrees with the Article 29 Working Party's recent suggestion that where EU-based data controllers conduct business and process data in multiple EU countries, applicable law should be based on the country-of-origin principle: only a single EU Member State's law should apply in such cases, rather than multiple (and often**

divergent) laws. For this to be achievable, however, it is essential that EU data protection rules are more fully harmonised.

- **Microsoft further supports the Working Party’s suggestion that the law that applies should be that of the data controller’s main establishment. In the context of cloud services, this should be deemed to be the market in which the provider’s primary data centre for processing applicable EU data is located. A similar regime should apply when cloud providers are positioned as data processors.**

The EU’s existing rules on applicable law – notably those contained in Article 4 of Directive 95/46 – remain vague and confusing, leading to inconsistent application across the different EU Member States and exacerbating the compliance challenges posed by divergences in national laws. The problem for online service providers, including cloud service providers, has been particularly acute. Under the current regime, providers that are established in or offer online services to users in multiple EU markets can find themselves required to comply not only with local DPA investigations concerning local data subjects (as they should be), but also with the data protection laws in each of those markets – laws that each in turn impose divergent obligations. This makes it difficult to develop and apply pan-EU policies and practices, and imposes significant compliance costs – without any corresponding benefit in terms of enhanced user protection.

Greater legal certainty in the application of EU data protection laws is required, both to protect the interests of EU consumers and industry. Microsoft notes that the Article 29 Working Party shares similar concerns, and supports the very positive contribution, expressed in the Working Party’s recent Opinion 8/2010 on Applicable Law, that the EU framework could be improved by adopting an applicable law rule for EU-based data controllers that mirrors the “country of origin” principle found in other legal frameworks, like the EU’s e-commerce rules. This refinement of current law will ensure that an organisation established in and operating across multiple Member States would need to comply with only a single EU Member State’s law, rather than a patchwork of multiple, different laws.

For this to be achievable, however, it is essential that the EU’s data regime be better harmonised at the national level; greater consistency across the EU should give national authorities confidence that the application of another Member State’s law adequately protects the personal data of their citizens. Otherwise, DPAs will be tempted to apply their local laws to data processing activities properly regulated under another state’s regime or organisations will have an incentive to conduct their processing in those countries with the lower levels of protection or imposing fewer regulatory burdens.

In terms of determining the relevant, single law to apply, we support the Article 29 Working Party’s suggestion that where a company operates across multiple EU Member States, the law applicable to its operations should be that of its main establishment. In the case of a cloud services provider or similar company, this would be the physical location of its primary data centre – defined as the EU Member State from where the provider directs its European processing operations, and/or has its physical infrastructure for processing data. We believe

that this approach largely accords with the views expressed by the Working Party, which stresses in Opinion 8/2010 that the main establishment of the controller actually involved in processing data, and not simply where the controller happens to be formally established, should determine the appropriate applicable law. Of course, national DPAs will still have jurisdiction to act when local data subjects' rights are involved.

Any application of applicable law to the cloud also must acknowledge the potential dual status of cloud service providers, which may qualify as both data controllers *and* data processors depending upon their particular relationship to data held in the cloud. To prevent cloud providers, when positioned as a data processor, from being exposed to the application of variable member state laws – albeit indirectly through their data processing contracts with their enterprise customers – we also would encourage the Commission to create an applicable law rule subjecting providers to the single law in the market of their main establishment. For this approach to be viable, it again would be necessary for any inconsistencies and divergences that currently exist among Member State data protection laws and governing the data processing activities of the provider's enterprise customers to be effectively eliminated.

D. Enhancing data controllers' responsibility (Section 2.2.4)

- **We agree with the Commission that the EU data protection framework must comprise more than simply prescriptive rules, and also needs to encompass measures that ensure European data controllers implement such rules and adhere to them in practice.**
- **Microsoft supports the Commission's suggestion that an accountability principle should be included within the EU framework. We encourage the Commission not to implement this principle simply by adding accountability elements as bolt-ons to the existing, prescriptive regime, however. Instead, accountability principles should serve as a flexible, yet robust, replacement for some of the more complex and rigidly formalistic aspects of EU data protection law.**
- **Microsoft also endorses the notion of "Privacy by Design" ("PbD") and the view that data protection principles be taken into account with the design and implementation of new technologies. Codification of PbD should not take the form of design mandates or technology preferences. Instead, the Commission should encourage technology providers to integrate core privacy principles, including data minimisation, transparency, and user control, into the development and deployment of new technologies.**

We agree with the Commission that EU data controllers need to embrace data protection as an important value in its own right, and put in place appropriate and effective measures to ensure that data protection rules are complied with in practice and subject to verification. In this regard, we welcome the Commission's suggestion that an accountability

principle be expressly included in the EU data protection regime. The adoption of an accountability principle should help to move the EU's data protection regime away from its current focus on compliance with prescriptive rules, and focus more on achieving substantive outcomes that enhance the levels of protection afforded to personal data.

This basic principle is not new. Accountability was included nearly 30 years ago in the OECD's 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; today, it finds expression in the Canadian Personal Information Protection and Electronic Documents Act, the APEC Privacy Framework and in other data protection regimes around the globe. The principle also appears in the privacy standards released at the conclusion of the 2009 international commissioners' conference in Madrid and meant to serve as a basis for a global privacy standard. In the EU's data protection framework, certain existing provisions of Directive 95/46, such as Article 17(1) and Article 6(2), impose obligations on data controllers that are aligned with the accountability concept. Unhelpfully, however, the principle of accountability has been variously formulated in these legal texts, making it challenging to define what it means precisely. Some legal frameworks see accountability as a mechanism to facilitate cross-border data flows, whereas others understand it as ensuring compliance more broadly.

Thus, at the threshold, it is vital that there be a shared understanding of the principle of accountability. We at Microsoft understand an accountability-based privacy regime to mean that data protection standards and requirements are enshrined in law, but that individual organisations are made more responsible for determining how best to meet those standards in practice. This approach places responsibility directly on the shoulders of the organisations that process personal data, mitigating the burden on individuals to police the use of their data (an obligation that is increasingly challenging in the new information economy). Accountability also means that the law moves away from simply trying to conform to prescriptive rules – regardless of their underlying purpose – and focuses on securing good substantive outcomes, in data protection terms.

Within Microsoft, accountability is a core component of our approach to data privacy, and permeates our own collection and processing of personal data, as well as our interactions with our business partners and vendors. We set ourselves a high standard of data protection based on legal requirements, self-regulation and best practices. We adopt a combination of measures that include policies and practices, technology, training and collaboration to achieve this standard – among them ensuring that privacy and data protections are systematically incorporated into the development and deployment of our products and services; providing users with clearly worded privacy policies; offering users tools to empower them to control their information online; and working with a range of online stakeholders to improve laws, strengthen self-regulatory mechanisms and create a more trustworthy online ecosystem.

We do have concerns, however, that the Communication appears to regard accountability as merely a “bolt-on” to existing prescriptive rules, when its great promise is in fact to act as a more flexible alternative to the proliferation of complex and potentially conflicting obligations. We strongly encourage the Commission to refrain from simply adding accountability-based obligations (such as requiring the appointment of a data protection officer

or the undertaking of regular compliance audits) on top of existing rules, and instead to consider using accountability in lieu of such rules (such as in the context of international data transfer, discussed in greater detail below in Section IV.A (Clarifying and simplifying the rules for international data transfers), or for national notifications). This approach will help to ensure that the EU legal framework is better equipped to respond to the challenges presented by modern computing paradigms and future technologies.

Notwithstanding the above, Microsoft does support the adoption of one particular accountability-based mechanism discussed in the Communication – so-called “Privacy by Design”. PbD is an integral part of how we conduct business and demonstrate accountability, and describes not only how we build products, but also more broadly how we operate our services and conduct our business. As part of our Trustworthy Computing initiative, we ensure that we engineer privacy into our products and online services at the outset of development; review all products and services to identify privacy issues at an early stage; help product groups follow Microsoft privacy policies and standards; and encourage the continued consideration of privacy and data security throughout the project lifecycle, including following the release of the product or service into the market.

Microsoft supports an industry-wide PbD obligation applicable to the ICT industry to take account of privacy principles, including notions of data minimisation, transparency, user control, use limitation, and related principles, in the development and deployment of new technologies. As with accountability generally, it is important that we reach a common understanding of what PbD entails, however. PbD obligations should not take the form of design mandates or technology preferences, for example. Indeed, it would be undesirable for privacy rules to dictate specific technological outcomes – including “privacy by default” – which will only impede the development of new technologies without guaranteeing stronger privacy protections. PbD obligations for any given technology should be proportionate to the privacy risks to the consumer; program assurance should place an emphasis on trustworthy internal checks and balances and limit reliance on third party audits and mandatory privacy certifications, which often impose significant costs with little concomitant benefit (to the extent external validation is necessary, it should be reasonable in scope and affordable); and there must be clear benefits for those companies that submit to higher levels of validation to demonstrate trustworthiness.

E. Encouraging self-regulatory initiatives and exploring EU certification schemes (Section 2.2.5)

- An EU-endorsed privacy certification scheme may help consumers to better understand and distinguish among the data protection practices of different providers. Any such scheme should be voluntary, affordable, technology neutral and capable of being rolled-out and recognised globally.**

Consumers can often be overwhelmed by the vast quantities of information regarding the many different ways in which their data is collected and used – making it difficult for

consumers to meaningfully understand and compare the approaches of different service providers to data handling and processing. Properly conceived, privacy certification schemes can offer a solution to this “information overload” by providing consumers with information in a consistent and efficient way. In doing so, certification schemes can enable consumers to better understand and distinguish among the data protection practices of online service providers, and can help them to make informed choices about which organisations to entrust with their personal data.

Certification schemes are generally best led by industry, via self-regulatory mechanisms such as those promoted in Article 27 of Directive 95/46. To date, very few EU-wide industry codes have been developed pursuant to Article 27, mostly because of challenges in securing regulatory buy-in. We believe that self-regulation plays an important role in ensuring strong privacy protections and we encourage the Commission to take a more active role in promoting these mechanisms.

If the Commission chooses to move forward itself with a privacy certification scheme, it should structure the scheme in a way that avoids unduly burdening companies – and particularly SMEs – with costly and bureaucratic obligations which discourage participation. Specifically, we recommend that the scheme should:

- *Be voluntary.* Mandatory certification schemes can chill innovation and deter competition in the development of enhanced privacy protections – just at a time when we are seeing an acceleration of innovation and competition in the privacy sphere.
- *Be affordable.* Some privacy certification regimes involve costs of upwards of €150,000 simply to certify one feature of a product or service – due largely to the requirement that independent third party auditors first evaluate the solution and make recommendations, which are then validated by the certifying entity. These costs create barriers to entry for all but the largest service providers, and discourage wide-scale use of the regime to the detriment of consumers. An alternative approach to consider could involve a self-certification regime, backed by possible audits conducted by privacy regulators.
- *Be neutral as to system, service or technology.* Similarly situated services and products should be subject to the same assessment criteria. Favouring some solutions over others creates market distortions to the detriment of competition and consumer choice.
- *Be capable of being rolled-out and recognised globally.* To help reduce the compliance burden on providers, any certification scheme should be capable of being endorsed by regulators outside as well as within the EU.

IV. The global dimension of data protection (Section 2.4)

A. Clarifying and simplifying the rules for international data transfers (Section 2.4.1)

- **The EU data protection framework’s rules governing international data transfers need to be revised, as well as simplified, to accommodate modern computing paradigms and anticipate future paradigms.**
- **To achieve this, Microsoft supports a solution where data can flow across international borders based on data exporters remaining accountable for the protection of the data regardless of geographic location.**
- **If the Commission remains committed to the current restrictive regime, Microsoft urges it to clarify that data transfers for specific, limited operational purposes can benefit from exemptions in the existing data transfer rules related to the performance of a contract.**
- **Further, the Commission should ensure that current data transfer mechanisms, such as binding corporate rules (“BCRs”), are streamlined and improved to provide for their more flexible and effective application.**
- **The Commission’s procedure for making formal, third country adequacy determinations also needs to be made more transparent and focus to a greater degree on ensuring that substantive protections are applied to transferred data.**

In today’s networked world, data knows few geographic boundaries. Instead, data travels regularly across national and regional borders – enabling many of the online services that we now expect and rely on as part of our daily lives. As the Commission is well aware, the rules within the EU’s data protection framework governing the transfer of personal data to third countries are often too rigid and inflexible to accommodate this reality, and need to be re-examined as a matter of priority. These rules, which are now over 15 years old, fail to reflect modern computing paradigms, the rapid explosion of the Internet and the increased delivery of online services to European consumers. If these rules are not adapted, they will ultimately obstruct the provision of online services to European consumers and will undermine the ability of EU businesses to compete in a global marketplace.

Microsoft favours an approach whereby data can flow across international borders based on data exporters remaining accountable for the protection of the data regardless of geographic location. As described in Section III.D (Enhancing data controllers’ responsibility), this would place responsibility on the shoulders of individual organisations that process data to determine how best to meet high standards of data protection. We believe such an approach would ensure the robust protection of data, but at the same time give organisations adequate flexibility to accommodate current data transfer needs. Appropriate accountability-based mechanisms for data transfer, an example of which includes BCRs, would need to be developed to suit the current – and any future – computing paradigms.

Accountability-based reforms would have the added benefit of enhancing consistency between the EU regime and some of the transfer regimes emerging in other major markets, such as in the APEC region. The APEC Framework now being developed by the Pacific Rim countries explicitly uses an accountability-based model, along with consent, for data transfers. It should be possible to achieve greater alignment between EU rules and such regimes without sacrificing levels of data protection or harming EU consumers. Global data flows are quickly becoming the norm, and it is therefore imperative that the EU's rules on data transfer embody a flexible, yet robust, approach that is capable of interacting with such regimes.

Alternatively, if the Commission remains committed to retaining the current restrictions on data transfers outside the EEA, we recommend at a minimum that the rules governing such transfers be reformed. Specifically, we would propose that:

- The Commission clarify that data transfers necessary to provide users with requested online services can benefit from existing exemptions to the data transfer rules – and in particular those that permit transfers related to the performance of a contract – in order to allow the free flow of data for specific, limited operational purposes (detailed below);
- More formal data transfer mechanisms, such as BCRs, be streamlined and improved to provide for their more flexible application; and
- The procedure for making formal, third country adequacy determinations be made more transparent and focus to a greater degree on ensuring that substantive protections are applied to transferred data.

We address each of these recommendations in greater detail below:

- Allow the free flow of data for specific, limited purposes

Helpfully, EU data protection law already contains some potentially useful exemptions to the normal transfer rules that are intended to facilitate data flows in limited circumstances, including potentially in online contexts. Microsoft believes that there is real scope for applying at least some of these exemptions in the cloud computing context. However, European DPAs have, to date, generally interpreted and applied these and any other exemptions in a highly restrictive fashion, and thereby effectively excluding their broader application in contexts where they might sensibly apply. We encourage the Commission to make these exemptions clearer and encourage their use in appropriate cases, which would include the cloud.

For instance, Directive 95/46 expressly permits data transfers to recipients outside the EU, without adequate protection, where those transfers are needed to conclude or perform a contract with or in the interests of the data subject. We believe that the Directive's contract related exception reasonably should encompass transfers for specific, limited operational purposes – enabling, for example, user authentication, service support and improvement, monitoring of service quality, and account/billing support, on the condition that the recipients agree to process the personal data under appropriate data protection principles. That said, this

outcome is unlikely in the absence of a revised statutory text or accompanying Commission guidance (possibly from the Article 31 Committee) to this effect given how narrowly regulators apply this and other exemptions in practice.

➤ Streamline and simplify existing transfer mechanisms

In parallel with these efforts, we also urge the Commission to focus attention on improving existing data transfer mechanisms, such as standard contractual clauses or BCRs, and better adapting them to modern computing practices. Often, these mechanisms can take weeks, months, or, in the case of BCRs, years to implement, hardly satisfactory where data can and needs to flow instantly across EU borders to deliver requested services to European consumers. Often, these timeframes are driven by the Member State data protection regulators themselves, who lack the necessary resources to promptly approve transfers, even non-controversial transfers using accepted transfer mechanisms; some DPAs, for instance, have been known to take up to nine months to approve the use of standard contractual clauses and, despite the best efforts of national regulators to adopt a mutual recognition scheme, only a handful of organisations (and to the best of our knowledge, no cloud providers) have secured regulatory approvals for their BCRs to date (and none have secured approvals across the entire EU).

Microsoft believes that these data transfer mechanisms can be simplified and streamlined, without diminishing the levels of protection afforded to transferred personal data, to accommodate today's networked world. The EU's BCRs regime, which offers a good example of the benefits that can be gained by incorporating the accountability notion into the EU framework, is a good case in point. BCRs easily could serve as a more flexible and less formalistic approach to data transfers, enabling data to remain adequately protected regardless of the recipient's location by means of robust internal policies and procedures, internal oversight and auditing, training and complaints handling, and related devices. In this way, BCRs serve as a good example of the benefits to be derived from the accountability principle, by focusing less on the means of transferring data and more on achieving the right outcomes in terms of the protections bestowed on personal data.

That said, the ability of BCRs to serve as an effective data transfer device has been handicapped by the cumbersome and inordinately slow administrative processes applied by data protection regulators to reviewing and approving BCRs. Despite the best efforts of regulators to expedite the process for granting approvals, taking the form of a mutual recognition scheme recognised by 19 Member States, it still takes months (if not years) for organisations to garner necessary regulatory approvals for their BCRs. To make BCRs more attractive and effective, the mutual recognition scheme needs to be expanded to include all Member States, such that a single regulatory approval can have effect in all countries. This would greatly diminish the current lengthy timeframes associated with BCRs.

Of course, once such approvals are obtained, it is then necessary to comply with the divergent local rules for implementing such approvals. In some cases, as in Belgium, this can even require procuring local ministerial decrees, leading to further delays. The fact that to date

only a few companies have secured approvals for their BCRs, despite their introduction in 2003, should be a concern. There needs to be a harmonisation of local rules relating to implementation, and, ideally, a process for fast-tracking implementation of approved BCRs. Further weaknesses with the BCRs regime include the fact that it only applies to intra-company transfers and can only be used by companies positioned as data controllers, rather than data processors, when transferring personal data. European organisations would benefit from such an expansion of its scope, making it more relevant to a wider range of data transfers than at present.

➤ Reform adequacy determinations

Microsoft also shares the Commission’s concerns over the process that now exists for making formal adequacy determinations vis-à-vis third countries. Clearly, adequacy determinations must be based on robust data protection criteria and involve a rigorous examination of those countries’ legal regimes. By the same token, the fact that the number of countries that have merited an adequacy determination in the past 15 years is in single digits suggests that the process is in need of urgent reform. Legitimate concerns have been expressed that the notion of “adequacy” has in practice been converted into one of “equivalency”, effectively excluding countries whose laws are not mirror images of the EU’s. And in cases where approvals actually have been granted, the adequacy analysis tends to concentrate on the existence of specific rules in third country regimes and the presence (at least on paper) of robust enforcement mechanisms – without delving deeply into whether a third-country’s regime actually succeeds in ensuring protection of data.

We believe that adequacy assessments should focus less on whether the regime being examined meets a list of prescriptive requirements, and more on the substantive outcomes it achieves. In this vein, the Commission should consider the possibility of granting sector-specific adequacy determinations, such that data of a certain type transferred to another country and subject to sector-specific laws or regulations, may be found to be adequately protected. For example, health and financial data transferred to the U.S. are subject to stringent regulation under U.S. laws, and the EU should be open to granting such “mini-adequacy” determinations in future. There is no logical reason why data transmitted under such circumstances could not also be “adequately” protected for purposes of EU law. Adequacy assessments should also be made more transparent to industry so that it can anticipate favourable determinations and put in place appropriate arrangements in advance of such determinations. At present, it remains unclear when and whether particular countries receive a favourable or unfavourable assessment.

B. Promoting universal principles (Section 2.4.2)

- **Divergent regional and national data protection and privacy regimes have prevented the emergence of a truly global data protection framework.**

- **If cloud computing and other emerging computing paradigms are to fulfil their potential, then a coherent international framework will have to be developed in the coming years.**
- **Industry is working hard to address these challenges, but we cannot succeed alone. Microsoft encourages the EU to assume a leadership role in forging a shared consensus on global data protection principles, working with its international partners and with industry, to arrive at flexible and robust data protection standards.**

European businesses operating globally must contend with an array of regional and national data protection frameworks that are poorly aligned, frequently inconsistent and often confusing. While various governmental and industry initiatives are underway to remedy the situation, a clear and comprehensive set of universally agreed rules and principles has yet to emerge and be embodied in domestic or regional laws worldwide. In the U.S., for example, a growing number of federal data privacy laws impose different rules for different industry sectors as well as for specific issues, including children’s online privacy, spam and telemarketing. Some countries in Asia, Africa and Latin America currently have no meaningful privacy frameworks, while others have implemented relatively sophisticated models of privacy regulation that attempt to cope with modern technologies and the online world.

Critically, the success of new and emerging computing architectures, foremost among them cloud computing, depends upon there being a coherent global data protection framework in place, with predictable and uniform rules. As the Article 29 Working Party has acknowledged, global standards regarding data protection are becoming “indispensable” in today’s networked world. Cloud service providers furnish services that transcend national boundaries, relying on data centres and infrastructure spanning multiple countries and regions. The data that they handle routinely originates in a number of different jurisdictions, flows across national borders and is stored in third countries. Because of the different data protection regimes in place, cloud providers are subject to a variety of sometimes inconsistent or incompatible rules and requirements. This makes it difficult for businesses to operate in this environment, and erodes user trust and confidence that their data is safe and secure.

Microsoft recognises that industry has an important role to play to address this challenge and to foster the emergence of a uniform and global data protection regime. As a leading technology developer and provider of cloud-based services for consumers and enterprises, Microsoft participates in various industry groups and initiatives whose aim is ensuring that appropriate rules are in place for addressing new technologies and critical issues like data privacy and security. For instance, we are a member of the Digital Due Process coalition, comprising privacy advocates, online companies and think tanks, which has urged the U.S. government to update the Electronic Communications Privacy Act to ensure that data stored in the cloud is subject to the same level of protection as data stored locally, possibly through enactment of a new Cloud Computing Advancement Act. In 2008, we helped form the Global Network Initiative, which remains dedicated to advancing Internet freedom and promoting transparency and user notice online. We also are actively involved with APEC, and

have lent our support to the APEC Privacy Framework and Data Privacy Pathfinder project. Through these and many other initiatives, Microsoft is working hard to find solutions.

But industry cannot on its own create the much-needed international framework, despite its best efforts. Policymakers and governments have a vital role to play, particular those in the EU given Europe's longstanding commitment to data protection and the status of data protection in the EU as a fundamental right. Microsoft urges the EU to take a leadership role in working towards a set of universally agreed data protection principles. Because the EU has a more advanced data protection regime than many other markets, and has experience addressing data governance issues at multinational (i.e., Union) level, the EU is well-prepared to exercise leadership on these issues along with the U.S. and other trading partners. The EU has already made notable progress in promoting shared principles with other trading partners: at the 2009 conference of international data protection regulators, data protection regulators from over 50 countries (excluding the U.S.) approved a Joint Proposal on International Privacy Standards (the "Madrid Resolution") in an effort to establish an agreed, international framework.

As a first step toward the long-term solution that is required, we urge the EU to commence discussions with U.S. lawmakers and regulators – as well as with industry from both markets – with the aim of agreeing a set of baseline data protection principles applicable to information stored in the cloud. A precedent for such an effort already exists, in the form of the EU-U.S. High Level Contact Group, which is now developing rules for transatlantic data sharing in order to fight terrorism and serious crime. U.S. authorities, such as the Federal Trade Commission ("FTC") and the Department of Commerce recently have been making strides in devising rules for regulating privacy online. The FTC released in December its long-anticipated staff report on consumer privacy, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers", and has offered preliminary recommendations for protecting consumers online. The Department of Commerce also has published its own green paper suggesting a new U.S. legal framework for addressing online privacy issues. These initiatives should offer fertile ground for opening up fruitful bilateral discussions between the EU and U.S. Ideally, these initial discussions will lead us on a path to more formal multilateral solutions – perhaps in the form of a treaty of similar international instrument under the aegis of the G8, G20, OECD or another international organisation.

V. A stronger institutional arrangement for better enforcement of data protection rules (Section 2.5)

- **Currently any organisation that operates and processes personal data across Europe has to deal with different national regulators who often will take different views regarding the organisation's obligations in relation to the same service; this is burdensome for business, confuses consumers, and leads to questionable privacy benefits.**

- **The Article 29 Working Party usefully could serve to better coordinate the activities of its member regulators; in parallel, greater transparency and more industry involvement in their activities is warranted.**

Microsoft supports efforts to improve cooperation among European DPAs, particularly in relation to cross-border activities. To the extent that DPAs react to, and seek to regulate, activities and services extending across multiple EU countries in an uncoordinated fashion, this presents a considerable challenge to business. It can require the same service to undergo multiple permutations in different markets, often confusing consumers and leading to questionable privacy benefits. We appreciate that the Article 29 Working Party has attempted to bring about more coordinated pan-EU action already, but those efforts have not proved successful.

Going forward, the Article 29 Working Party usefully could serve to better coordinate the activities of its member regulators. In addition, we believe that the operations of the Working Party should be made more transparent through measures such as engaging in more dialogues with stakeholders and opening certain Working Party discussions and debates to the public. We also encourage the Working Party to engage more actively with industry in formulating its positions and generating opinion papers and working documents to ensure that they remain fully informed and accurate as possible. One way to increase industry engagement would be to include industry representatives in Working Party expert groups on specific issues. This is especially important where opinion papers disproportionately impact an industry sector or particular company or companies, or where the Working Party is focusing on technology related issues, where sophisticated technical input is often essential.

Finally, we also support efforts to ensure that national DPAs in Europe are appropriately staffed and adequately resourced. With additional resources, authorities may be able to take a more active role than at present in educating both industry and individuals on data protection requirements and good information handling practices.