**Microsoft response to the Ministry of Justice Call for Evidence on EU Data Protection Proposal - Regulation COM(2012)11**

**6th March 2012**

## Executive Summary

Microsoft welcomes the very idea of a "Regulation" since a consistent framework across the EU is essential for the development of growth and innovation in the EU.

We also support the European Commission's goal that companies will be subject to a single supervisory authority based on their country of "main establishment" ("one-stop shop" approach). However, the Regulation should clarify rules and refer to the physical location of an entity's primary data center to ensure that there is a close and effective link between the market where data is processed and the Data Protection Authority (DPA) supervising the data processing.

The Regulation introduces many new "rights" to data subjects. While Microsoft supports strong privacy enforcement for the benefit of consumers, many provisions are not technically practical to implement. It is important to also grant incentives to data controllers/processors and encourage good practices by rewarding those that demonstrate responsibility by adopting particularly rigorous data protection programs.

Microsoft is concerned that an unrestricted secondary rule making process can result in excessive regulatory overheads. The European Commission should focus on "what", instead of defining "how".

**Introduction**

Microsoft is pleased to respond to the Ministry of Justice's Call for Evidence on EU Data Protection Proposal - Regulation COM(2012)11 ("the Regulation") and we look forward to working with you to ensure that the final Regulation is one which supports the growth of the UK economy.

Microsoft welcomes steps to strengthen and harmonise the data protection regime. Our company's greatest asset is customer trust and our technologies are developed with data protection in mind. Our priority is to protect personal data in an age where we support ubiquitous connectivity, pervasive online business and social networking, and flows and storage of information all over the world on all kinds of devices.

Our efforts have led us to conclude that enterprises, including Microsoft, have a critical role to play in protecting privacy – a role that includes embedding privacy protection into products and services early in and throughout the design cycle, and being transparent about how we collect and use data. With this in mind, we have invested heavily to provide clear and easy-to-understand guidance about how we gather, store, manage and secure information.

It is clear, however, that the dramatic technological changes of the past decade have tested Europe's existing data protection framework. While the explosive growth of the internet has brought us tremendous social and economic benefits, internet technologies have also fundamentally expanded how, where and by whom data is collected, transmitted and used. The rapid growth of cloud computing is a prime example. Attracted by the significant cost savings and flexibility of cloud services, individuals, businesses and governments are storing and sharing unprecedented amounts of information online, leading to a significant increase in the quantity and types of data collected and processed by third parties. Cloud technologies offer great promise for Europe, with estimates indicating that the cloud will create a million new jobs and several hundred thousand new small- and medium sized enterprises, and drive down the cost of ICT for the public and private sectors. But these and many other web-enabled benefits will only be realised if users have confidence that their personal data and the data they process for others are safe in the cloud.

The Regulation adds a number of important measures that will help to achieve these goals, including requirements that companies design technologies with privacy in mind, be transparent about their processing activities, and remain responsible for how they use personal data. The proposal also helpfully addresses inconsistent rules and interpretations across the 27 EU Member States, reduces the administrative paperwork for companies, and improves mechanisms to transfer data safely outside of the EU.

Other proposals – particularly those relating to online technologies – need refining to ensure that the protections they offer are both strong and workable. For example, the Regulation in some places dictates not only what obligations apply, but also how those obligations should be implemented – moving the Commission beyond creating regulation to support privacy and into designing technology and business processes. Overly prescriptive approaches in areas like a "right to be forgotten", data portability, and consent do not always reflect how the internet is technically structured today, what

consumers want and need, or how technology is likely to evolve tomorrow. Obligations that cannot be properly implemented due to technical hurdles, or that frustrate data subjects, or that become obsolete when technology changes, will increase operating costs for businesses but will be of little lasting value.

**1. Cost of the Regulation**

The European Commission has claimed that the Regulation will cut costs and cut red tape and will save European business €2.3 billion per annum. We believe that the evidence for this claim is not compelling. It is our belief that the Regulation, as currently drafted would increase costs for the businesses that will have to comply with it. The current proposal also increases liability risks for companies, potentially leading to slow down in small and medium enterprises that are engaging in internet related ventures in EU. It is however, difficult to determine exactly what the quantifiable costs of compliance with the Regulation are likely to be for Microsoft, especially since the European Commission will be able to promulgate an extended set of secondary rules. The types of direct and indirect costs that Microsoft currently bears in complying with the current data protection regulation include assessment and audit, regulatory analysis, specialised technologies, training, certification, and legal and other vendor related costs. All of these costs could potentially rise as a result of many new requirements proposed in the new regulation.

Although data on the impact of compliance with the Data Protection Regulation on Microsoft's business activities is currently unavailable, we note the general data available on the cost of compliance with data protection rules. In January 2011 the Ponemon Institute LLC published a study which looked at a representative sample of 46 multinational companies, from SMEs with less than 1,000 employees, to companies with more than 75,000 employees. The study sought to determine the full economic impact of data-protection related compliance activities. It found that a company with more than 75,000 employees typically spends about €7 million on privacy compliance. It should also be noted that cost of compliance on smaller businesses could be proportionally higher than larger companies. In order to drive economic growth in EU and keep it globally competitive, it is essential that regulatory environment does not impose cost prohibitive burdens on businesses.

We are also concerned that many of the provisions introduced in the Regulation are vague, unclear, and perhaps, technically impractical to implement. Any confusion and regulatory uncertainty adds to a business's costs. These points require clarification so we have expanded upon this issue for specific examples in the text below. Lastly, the administrative sanctions (up to 2% of annual turnover) which a data controller could be subjected to if they fail to comply are disproportionate to potential harm and may create a chilling effect on industry in the EU. We would also like to see a better definition of the circumstances and processes that will be taken into consideration for the levy of the fine.

**2. Secondary Legislation**

The Regulation significantly increases regulatory uncertainty for Microsoft. We are particularly concerned about the broad range of areas in where the European Commission has the power to adopt secondary rules. Our concerns are that this could lead to over-regulation and/or technology mandates. Furthermore, the process of secondary legislation (recently reformed in the Lisbon Treaty) is largely new, could take a long time to implement and it is difficult to predict the scope for stakeholder involvement. The Commission's ability to propose secondary legislation in a wide number of areas threatens to complicate, rather than simplify, data protection. If new rules are regularly adopted, it effectively means that the benchmarks for data protection are always changing and it becomes virtually impossible for enterprises ever to achieve compliance, increasing costs for businesses. Moreover, if the Commission chooses to adopt highly prescriptive measures or dictate specific technology outcomes via delegated and implementing acts, this could potentially hinder innovation in privacy protection.

Rather than seeking to promote greater harmonisation through the adoption of secondary rules, we believe it would be better to rely on other harmonising mechanisms already in the Regulation, such as the single supervisory authority, the European Data Protection Board, and mutual assistance and joint operations among national regulators. At a minimum, the Regulation should make clear that any secondary rules do not take the form of design mandates or preferences for particular technology solutions.

**3. Main establishment**

Under current EU law, companies with a presence across Europe often need to address multiple, and sometimes divergent, national data protection regimes. The Regulation meets this challenge by proposing a single law for Europe and by setting a goal that companies processing data in the EU will be subject to a single supervisory authority based on their country of "main establishment."

Yet the Regulation defines "main establishment" in a way that may add to confusion rather than reduce it. For example, to determine a processor's main establishment, the Regulation looks to the place of "central administration" – a term that is undefined and in practice may have no relation to the market where data is in fact processed. The Regulation uses a somewhat more sensible test for controllers, based on where "main decisions" about processing are taken in the EU – but then introduces an unclear and circular test relating to "main processing activities" in the context of an establishment. The result may be that multiple data protection authorities claim jurisdiction over organisations, especially organisations that act as both processors and controllers in multiple Member States.

We would recommend a common-sense, simple approach that (i) applies across the board to controllers and processors alike, and (ii) defines "main establishment" by reference to the physical location where the controller/processor has its primary data processing facilities). This approach ensures that there is a close link between the market where data is processed and the DPA supervising that processing.

**4. The role of data processors**

The Regulation increases the obligations on processors. While increased obligations in some areas may be warranted, these new responsibilities should reflect both the complex contractual environment in which processors operate and the limited control they often exercise over data they are processing. For example, the Regulation requires that processors grant supervisory authorities access to data in certain circumstances – apparently regardless of any competing contractual obligations. The liability of processors also increases under the new regime. These and other aspects of the balance in responsibilities between controllers and processors should be carefully considered in light of contractual obligations already imposed on processors, in order to avoid potential contradictions stemming from overlapping responsibilities.

The Regulation could also be clearer in terms of the dividing line between processors and controllers. With the evolution of technologies like cloud computing, the distinction between processors and controllers can sometimes blur. While the Regulation does seek to clarify these roles, further guidance and precision in this regard would be useful. Because the Regulation applies different tests and obligations to controllers and to processors, it will be essential for enterprises to understand clearly when they are controllers and when they are processors. For example, as noted above, the Regulation proposes different tests for "main establishment" for controllers and processors; if an enterprise is not clear on the role it is playing, it cannot determine which test applies or identify its supervising DPA.

**5. Right to be forgotten**

Under Directive 95/46, data controllers have the obligation to erase personal data at the direction of the data subject in certain scenarios. The Regulation builds on this principle by giving individuals a "right to be forgotten" (RTBF). As conceived in the Regulation, the RTBF would not only require companies in certain circumstances to erase personal data upon a request from the data subject, but also, where that data has been made public, the company involved would be required to inform any third parties processing that data about the request to erase copies of or links to that data. The Regulation imposes harsh penalties on controllers that fail to comply.

The structure of the RTBF does not fully reflect the structure of the internet. Digital data today is often quickly replicated across the web on systems and servers across the globe with or without any formal technical or contractual relationships between different parts of the online ecosystem. For example, many search engines and content aggregators use publicly available internet information to catalogue and build large caches of data without any explicit contractual agreement with the primary publisher of the information. These caches are what make it possible for individuals to find data quickly on the internet when they do an Internet search. However, as a result, it can be difficult if not impossible to "remove all tracks." By requiring that controllers notify any and all third parties, the RTBF provision seems to envisage that companies can oversee the entirety of the World Wide Web and control the

information on it – an obligation that is directly at odds with the open architecture of the internet. Indeed, European law (in the E Commerce Directive) already recognises that it would be unreasonable to ask companies to monitor the internet and makes clear that companies should not be required to do so.

To be workable, any interpretation of the RTBF must not obligate companies to do that which is technically impossible. Accordingly, the Regulation should limit the RTBF to that data retained by and under the control of the controller and reasonably accessible in the ordinary course of business. At the same time, the RTBF should extend only to a user's own data (i.e., data that a user inputs directly) and not to data generated in the operation of the service (for example, error messages or uptime statistics). And to help protect users, service providers should be permitted to retain data for a limited period in order to re-enable accounts that have been mistakenly or maliciously deleted.

**6. Data portability**

With the increasing use of online services, social networks and cloud technologies to hold all sorts of personal data, it has become increasingly important that users are able to take their data with them when they leave a service. The Regulation seeks to ensure this by proposing that individuals be able to "port" their data. But the Regulation goes beyond this, and requires that the data be returned to users in a way that allows for a direct transfer to other services. The Regulation also gives the Commission the power to impose technical standards governing the format in which data is to be returned.

Microsoft absolutely supports giving individuals more control over their data – increased data mobility is not only good for users, it is also good for business and the overall ecosystem. But the Regulation should recognise the technical reality that the ability to export data does not necessarily mean that such data can be used "as is" in other services. Companies use a wide range of mechanisms to enable the export of data – among them industry standard formats, import/export functions and application programming interfaces (APIs) permitting others to connect to the data directly – depending on the technology, service and functionalities involved. And new mechanisms are invented every day. As a result, the successful transfer of data from one service to another is not a simple proposition – and mandating a single format for data transfer will require technology providers to change other aspects of their products and services which may result in increased business costs, less functionality, less diversity and a worse overall user experience.

We propose a solution that permits users to port the data they had originally created, but allows industry to decide on formats and technical details of returning user data back to users, based on a variety of technical and commercial factors – including an emphasis on ease of use and the prevalence of a particular format and method.

**7. Certifications**

The Regulation helpfully promises to promote certifications and other mechanisms to encourage organisations to demonstrate their security and privacy commitments. Microsoft welcomes such efforts and has been at the forefront of pursuing many industry leading certifications. However, Microsoft would like to encourage the Regulation to support international certifications, including EU-adopted international certifications, instead of sector-specific or regional certification programs, which can lead to fragmentation of standards in privacy and data security. Industry with other relevant stakeholders should be deeply involved in developing the certifications so their expertise is incorporated, with oversight and help from the Commission.

**8. Data breaches**

Data breaches are a recurring challenge to individual privacy. A breach notice obligation is thus key to ensuring that DPAs and data subjects are informed and can take appropriate measures where serious breaches threaten significant harm.

As crafted, however, there is a real risk that rather than promoting good practices, the breach notice provisions in the Regulation will discourage them. For example, the Regulation does not include any threshold test for when DPAs must be notified about a breach. Instead, the Regulation requires all controllers in all sectors to notify DPAs about all breaches, regardless of their gravity, within 24 hours; failure to comply exposes a controller to penalties up to 2% of worldwide turnover, even where that failure is simply the result of negligence.

Under this regime, DPAs may quickly find themselves overwhelmed by notifications, impairing their ability to effectively tackle the truly serious breaches – a problem that will be compounded by the 24 hour deadline, which will lead controllers to notify suspected breaches even in cases where further investigation would have demonstrated there was in fact no breach. And while the Regulation does include a threshold for notifying data subjects (i.e., when a breach is likely to cause an "adverse effect"), the threshold is so low that it means data subjects will likely receive constant notifications – inducing "notice fatigue" and leading consumers to ignore breach notices. Excessive notices may also lead to an unreasonable level of fear among European internet users, which may negatively affect the use of internet based technologies.

To ensure the regime is effective, controllers should be required to notify data subjects and/or regulators of a breach only when there is significant risk of serious harm to the data subject. Criteria to be considered in making this assessment could include the type of data involved and its sensitivity, the nature of the breach, the number of data subjects affected, and the type of harm threatened by the breach. Also, consistent with the breach rules in the 2009 additions to the e-Privacy Directive (2009/136), companies should be required to notify DPAs "without undue delay" rather than within a 24 hour window. And severe penalties for non-compliance should be reserved for those controllers who wilfully and repeatedly fail to notify.

**9. Consent**

The Regulation permits controllers to process personal data where the data subject has consented to the processing. To ensure that this consent is meaningful, the Regulation includes a number of important safeguards, among them requirements that consent be freely given and informed, and that companies clearly distinguish requests for consent when those requests are part of broader communications with customers. But in addition to these safeguards, the Regulation also prescribes that consent must be given in one way – i.e., "explicitly," and by either a "statement" or "clear affirmative action by the subject" – no matter the context in which consent is obtained or the data is used.

As drafted, the need for consent to be explicit could be read to require that controllers operating online force users to affirmatively "opt in" to the use of their data. We believe that this "one-size-fits-all" approach is too narrow. There is currently a wide range of mechanisms that effectively enable users to control and consent to collection and use of their information depending on the circumstances involved. By preferring one mechanism over others, the Regulation diminishes the incentives to develop different and potentially better privacy protecting solutions.

Equally important, by requiring users to opt in to every use of their data, the Regulation will potentially require internet users to opt in dozens of times, if not more, during a single web surfing session or mobile internet use. Yet consumers demand internet services that are fast, easy-to-use and efficient. Onerous and static opt-in mechanisms instituted by controllers will frustrate many users – and ultimately may lead users to opt in as a matter of routine, even in cases where their privacy would be better served by opting out.

Companies relying on consent to process data should be required to ensure that consent is informed and meaningful – and this the Regulation does. But the Regulation should also permit innovators to use different mechanisms to obtain consent that reflect how and in what contexts consent is obtained and data will be used.

The Regulation, like the 95/46 Directive, also permits some processing of personal data even when consent is not obtained (for example, under the legitimate interests exception). We welcome this as in some cases consent places too high a burden on the data subject to understand all uses of their information in an ever increasing complex arena of data flows. As with the comments above on profiling, the Regulation should carefully view what uses of data are appropriate and may be permitted even where express consent is not obtained.

**10. Responsibility**

Drawing from the international concept of "accountability," the Regulation will require controllers and processors to be "responsible" for how they handle data. For example, the Regulation requires organisations to appoint a data protection officer responsible for compliance. Privacy impact

assessments (PIAs) are another important part of being a responsible data steward, and the Regulation usefully clarifies that companies should carry out PIAs when processing operations "present specific risks to the rights and freedoms of data subjects."

These reforms, and others like them, will help keep data safe. But we believe that certain changes will help to make these responsibility obligations even more robust. For example, with regard to PIAs, the Regulation stipulates that controllers and processors must seek the views of data subjects when conducting PIAs, and consult with supervisory authorities prior to processing the data in those cases where a PIA "is likely to present a high degree of specific risks." In this scenario, DPAs and data subjects could soon find themselves overwhelmed by PIAs (Microsoft alone undertakes over 2000 PIAs each year). Moreover, mandating the disclosure of PIAs could change the nature of privacy assessments by making companies less candid in their evaluations; mandated disclosure could also undermine the protection of data by creating risks to the confidentiality of information. We thus recommend that these requirements be eliminated. At a minimum, we would welcome greater clarity as to exactly when these rules apply to processors; such clarity is essential, particularly because the Regulation subjects even negligent non-compliance to harsh penalties.

In addition, more broadly, we believe it is important to motivate companies to be responsible by providing clear benefits for doing so. The new regime should encourage good practices by rewarding organisations that demonstrate responsibility and adopt and validate particularly rigorous data protection programs. One way to do this would be to allow organisations that have demonstrated themselves to be responsible – for example by implementing global data protection standards such as ISO 27001 or 27002 – to transfer data across international borders with reduced administrative requirements.

**11. Data protection by design and default**

The Regulation also proposes an industry-wide "privacy by design" (PbD) obligation – another integral part of responsibility. Microsoft believes strongly in PbD. Microsoft works hard to 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 product lifecycle.

We strongly support a PbD obligation. We also welcome the fact that rather than dictate in prescriptive terms how PbD is to be implemented, the Regulation instead dictates the outcome that enterprises must be achieve – leaving technology providers free to innovate so long as their innovations protect privacy. Consistent with this approach, we also recommend that express language be added to the Regulation making clear that when the Commission adopts delegated and implementing acts in the area of PbD, this legislation should not take the form of design mandates or technology preferences. Mandates and preferences only serve to impede the development of new technologies, with no guarantee of stronger privacy protections.

Importantly, in addition to PbD, the Regulation also includes a new and vague obligation requiring controllers to implement mechanisms to ensure that by default they process only data that is necessary for each specific purpose of processing. The intention here may be well founded – we recognise that default settings play an important role in protecting privacy. But, in practice, it is unclear what this obligation entails. This lack of clarity creates uncertainty and, combined with the possibility of the Commission setting "technical standards" in this area, could have unintended negative consequences, such as impairing innovation, limiting functionality and creating user frustration. We would recommend instead that, as part of PbD, the Regulation encourage innovators to assess the full universe of potential privacy risks and make appropriate decisions about privacy designs and settings.

**12. Enforcement**

Robust rules on the books are a key element of a strong data protection regime. But effective enforcement of those rules is equally important to ensure that companies take their responsibilities seriously. Supervisory authorities should be granted the power to impose meaningful sanctions for flagrant or repeated violations that threaten real harm to the individuals affected.

Consistent with this view, the Regulation includes strong sanctions for violations. But less helpfully, the Regulation again takes a "one-size-fits-all" approach, and could be read to apply the same sanctions to deliberate, flagrant violations of the rules as it does to violations that are merely accidental. This means that a company that inadvertently fails to use a specific electronic format when giving a customer access to his information could face the same penalty as a company that repeatedly and intentionally collects and processes data about individuals without informing those individuals about its activities.

At the same time, the Regulation also could be read to restrict the discretion of DPAs by requiring them to impose penalties. Specifically, the Regulation might require that where a violation has occurred, DPAs must impose a fine – even where that violation may not, in the eyes of the responsible authority, merit one. Any automatic assessment of penalties will inhibit companies from self-reporting, reducing overall transparency, security and privacy. This approach may have a particularly chilling effect on small- and medium sized European internet based businesses.

To be balanced and effective, the Regulation should ensure that the most punitive sanctions are reserved for truly bad actors. This requires that DPAs be given the authority to impose sanctions only where truly warranted. It also requires that unintended missteps be subject to separate and lesser penalties, and that there are clearly-established "aggravating" and "mitigating" factors that guide when a penalty should be at the high end of the range and when a penalty should be at the low end. While the Regulation identifies some factors that DPAs should consider in assessing fines, the list is not comprehensive. In the context of data breaches, additional factors could include, for example, the sorts of measures the company involved took to avoid the breach, whether the company was genuinely uncertain about whether the activity constituted a breach of relevant obligations, and if the organisation took steps to remedy the breach immediately upon becoming aware of it.

**13. Profiling**

The use of the internet and the proliferation of connected devices generate unprecedented levels of data – which can sometimes be used to build profiles. Profiling itself is merely a technical process that helps identify patterns across large quantities of data, and in doing so allows information to be collected and organised in meaningful ways. As such, there is nothing inherently wrong with profiling. Indeed, profiles are frequently used to satisfy consumer demands for technologies and services that remember their preferences, such as their native language or home country, or that are customised in other ways.

Of course, as with any business process, automated profiles can also be used to achieve less desirable outcomes, such as discriminating against individuals on the basis of their health. To ensure that user data is not used to achieve goals that are contrary to EU citizens' interests, it makes sense to regulate the use of profiles for harmful purposes. However, such rules should not restrict the building of profiles for all purposes – including beneficial purposes that are intended to respond to legitimate consumer demands.

The robust protection of data subjects will be better served if the Regulation focuses on how profiles are used, instead of on the mechanisms used to create profiles. The Regulation should be amended to make clear that profiles can continue to be used for beneficial purposes such as providing customised internet experiences to users.

**Contacts**

For more information, please contact becky.foreman@microsoft.com or donna.whitehead@microsoft.com.