16 October 2012

Mr Jan Albrecht
Member of the European Parliament
Brussels

Re: EU Data Protection Regulation

Dear Mr Albrecht,

We, the undersigned organizations, provide the following comments as uniform input into the legislative review process currently being undertaken of the draft General Data Protection Regulation formally proposed by the European Commission on 25 January 2012. Business shares with government the desire for data protection regulation that accomplishes the twin goals of providing for effective protection of personal data and privacy while enabling the data flows that are needed by new technologies and business models to foster both economic growth and societal benefit in Europe and globally. We also wish to recognize and applaud the commitment to multi-stakeholder consultation that has been evidenced by the EU, the US and other countries in their consideration of data protection issues and development of policy and regulatory instruments.

The topics outlined in this letter represent a high-level consensus among all the undersigned organizations of important considerations which should be taken into account in the review of this draft Regulation, both to ensure the intended benefits and to ensure that other requirements, as drafted or further elaborated in delegated or implementing acts, do not create undue burdens for business or data protection authorities (DPAs) or unintended consequences. While seeking to enhance the fundamental right of the protection of personal data, an overall objective of the new data protection rules must be to not unduly constrain innovation, hamper economic growth, limit the competitiveness of the EU economy or otherwise diminish the potential for societal benefits of new or established technologies and business models. We believe this balance is not yet achieved and the current text considerably adds additional burden for businesses. The draft regulation lacks a risk-based approach to data protection and does not appropriately recognize the need to more carefully consider the context of application or the varying consequences of

failures of protection. All data is not equal and should not be treated as such. For the majority of the changes being proposed, there is no indication as to why the high level of protection under the existing data protection framework should have to be increased any further. To strike an appropriate balance we suggest the following.

High-level Recommendations for Review of the Draft Regulation:

1. Reduced administrative burdens: While the choice of instrument, a Regulation, stands to harmonize applicable law for the protection of personal data across the EU, it is essential that provisions pertaining to jurisdiction, in particular the concept of the lead supervisory authority, are clarified, strengthened and implemented in a practical fashion. Business considers clarity over applicable law and jurisdiction to be key benefits to the revised rules and essential to the endorsement of the Draft Regulation.

2. Practical operational requirements: The need to ensure that operational requirements for organizations are practicable, not unduly burdensome, take cost appropriately into account and do not result in unintended consequences that could constrain growth, benefits or innovation. Some of the most important issues include:

    - The range and specificity of detail required of documentation which could create significant and needless burdens. These requirements need to be flexible to address different business models and levels of data risk for different businesses.

    - The number of Data Protection Impact Assessments (DPIAs) required: their content, scope and need for prior notification or approval which could needlessly increase cost and unduly constrain both innovation and the timely provision of services.

    - The scope of the definition of breach and associated notification requirements, especially the concepts of notification within a reasonable timeframe, mitigating effects of safeguards (encryption, etc) and potential for harm or adverse impact which pose issues of practicability and undue burden.

    - The limited practicability of the right to be forgotten beyond the site collecting the information.

3. Clarity and predictability: The need for clarity and predictability in the requirements and their implementation. Issues for consideration include:

    - The need to recognize that harmonization and predictability relate to how the Regulation will be applied and do not imply the need for overly detailed and prescriptive requirements.

    - New independent obligations on processors, which would create confusion as to obligations and responsibilities between controllers and processors, should be reconsidered in favor of better applying existing requirements.

    - The need for further guidance on the potential development of certification, Privacy by Design and Privacy by Default concepts, and the appropriateness of their inclusion in a Regulation.

- The overuse of the provision for delegated acts and the failure to scope or limit the nature or potential impact of the delegated acts or provide for stakeholder consultation related to their practicability and impact.

4. Proportionality, cost-effectiveness and competitiveness: The need to increase consideration of proportionality, cost-effectiveness and competitiveness. Issues for consideration include:

    - The need to review the alignment between the recitals stating the objectives of the Regulation, broadly supported by Business, with the requirements set out in the articles which are often more problematic. Overly prescriptive requirements inhibit the goal of the Regulation to be technology neutral and to reflect appropriate compliance for different business types i.e. data focused models such as social media companies vs. businesses which process only employee and business contact details.

    - The need to consider the potential negative implications, both for the protection of personal data and for the development, whether by government or the private sector, of new and existing services, of an overbroad definition of personal information, an overly strict and inflexible approach to "consent" or excessively strict limitations on profiling which could affect the legitimate interests of data controllers.

    - While there is a general recognition of the need to enhance credible enforcement mechanisms, specifically sanctions and fines, the current proposal lacks proportionality and may make the EU less competitive in attracting investment in facilities or services without necessarily adding to the protection of personal data and privacy. Furthermore, the mandatory nature of the fine may not allow mitigating factors and the context of the acts to be properly taken into account. Other sanctions, such as specific performance, may be more effective and appropriate than fines, and DPAs need to have discretion to enforce based on the facts of each case.

5. Interoperability of privacy frameworks: The need to consider opportunities for facilitating responsible global information flows by evaluating interoperability of EU frameworks with those outside the EU. European and global companies have a substantial economic need for cross-border data flows between countries and regions with very different privacy regimes. An interoperable international privacy regime that recognizes differing privacy rules (such as the US multi-stakeholder process) to the greatest extent possible, and honors these rules, would greatly accommodate companies operating in multiple jurisdictions and facilitate global economic growth. Topics for consideration could include:

    - While specific inclusion of Binding Corporate Rules (BCRs) is welcome, BCRs for processors and the ability to use BCRs across groups of companies would enhance the utility of BCRs in the cloud and other global environments.

    - Guidance of how codes of conduct, sectoral adequacy, appropriate safeguards and legitimate interest may be used as a basis for transfers would ensure that businesses can optimize responsible information transfers in ways that comply with the draft Regulation.

6. Clarification of "Profiling": The need to ensure that the provisions relating to "profiling" do not prevent businesses from being able to evaluate and analyze data and use such data

predicatively for legitimate business purposes, including identity verification and fraud detection and prevention. Additional issues for consideration include:

- Clarification of the phrase "measures based on profiling" to make it clear that legitimate business uses of data will be permissible.
- Clarification of the terms "legal effects" or "significantly affects" as applicable to "profiling" and how permissible uses of data are otherwise limited.

The topics presented above represent a consensus among the undersigned organizations of important issues that need to be addressed in the review of the draft Regulation. The undersigned organizations will, as appropriate to their membership and expertise, provide more detailed comments outlining substantive concerns and suggested resolutions to those concerns as well as more specific topics which may be more directed at specific sectors of types of services.

We look forward to working with the EU Council, Parliament, Member States and the Commission in the further enhancement of the Regulation. We seek to ensure the continued and effective protection of personal data and privacy while also ensuring that Business can remain innovative and flexible in using the new technologies and business models to enhance continued economic growth, societal benefit and EU competitiveness.

Sincerely,

Susan Danger
Managing Director
AmCham EU

John Higgins
Director-General
DIGITALEUROPE

Kristen Verderame
Interim President & CEO
European-American Business Council

Ken Wasch
President
Software & Information Industry Association

Peter Robinson
President & CEO
United States Council for International Business