AMCHAM EU
AMERICAN CHAMBER OF COMMERCE TO THE EUROPEAN UNION
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

AmCham EU position on the General Data Protection Regulation

POSITION STATEMENT

11 July 2012
American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
Email:info@amchameu.eu

Secretariat Point of Contact: Roger Coelho, roger.coelho@amchameu.eu, 32-2-289 10 18

This document sets out the position of the American Chamber of Commerce to the European Union (AmCham EU) on the European Commission's proposed General Data Protection Regulation. The document incorporates and builds on our responses to previous Commission consultations on the European Union's approach to the protection of personal information.[1]

AmCham EU is comprised of 140 companies from a wide range of sectors with operations and employees across Europe. Our members are committed to a strong data protection framework and believe it is essential to gaining and keeping consumer confidence in our businesses, products and services. From first-hand experience we know that balanced, workable data protection rules are critical to enable innovation and economic growth.

In this context AmCham EU welcomes the review of Directive 95/46/EC, which presents the EU with an unparalleled opportunity to craft a state-of-the-art data protection framework to better protect Europe's data subjects, eliminate unnecessary burdens on controllers and processors, and promote international harmonisation by serving as a model for third countries.

Because of the complexity of this issue, we have summarised our key points below in this position paper and have provided more detailed analysis of the proposal and our recommendations in the accompanying Information Paper. Broadly, our views are as follows:

- **AmCham EU applauds the Commission's efforts to create one law applicable to all member states.** Today, companies in Europe effectively operate under 27 different national regimes. This environment creates legal and business uncertainty. The Regulation goes a long way toward clarifying applicable rules and creating a 'one-stop-shop' for compliance. But eliminating uncertainty entirely will require the Regulation to go further and include language to ensure that a single, enterprise-wide interface with compliance authorities is possible. Among other changes, the number of delegated acts needs to be reduced and clear timetables must be introduced for their adoption. In addition, the responsibilities of supervisory authorities must be further clarified.

- **To reflect the complexity of modern data processing, AmCham EU recommends that the Regulation avoid a 'one-size-fits-all' approach; instead, rules need to be flexible to adapt to different circumstances while at the same time respecting the principle of technology neutrality.** There are many different types of data, and many different ways of collecting and using data. Some data practices raise privacy concerns, while others do not. The Regulation's rules -- including rules relating to how personal data is defined, how consent is obtained and when profiling is permissible -- should be flexible enough to accommodate these varying contexts.

[1] See AmCham EU's response to the Commission communication on a comprehensive approach on data protection in the European Union, 14 January 2011; AmCham EU Position Statement on the Commission consultation on protection of personal data', 19 January 2010; and 'AmCham EU response to the Commission consultation on protection of personal data', 19 January 2010, www.amchameu.eu.

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE TO THE EUROPEAN UNION
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

POSITION STATEMENT

- **We are also recommending changes to the proposed Regulation to ensure that it strikes the right balance between protecting personal data and enabling innovation in technology and business models.** Rules relating to the right to be forgotten, data portability privacy impact assessments, and privacy by design and default, among others, must leave industry with the required flexibility to continue to create innovative solutions to challenges facing business and consumers while at the same time ensuring that users can exercise meaningful control over their own personal data. Currently, these rules appear to be overly prescriptive.

- **To make sure Europe remains a desirable place to do business, the Regulation must enable cross-border data flows in keeping with the needs of the information age.** Replacing the proposed ex-ante approach with an accountability-based transfer regime that requires controllers and processors to protect information wherever it is held would help to achieve this objective. If that proves too radical, however, the transfer mechanisms proposed in the Regulation -- including Binding Corporate Rules (BCRs), standard clauses and derogations -- must be carefully considered to ensure that they work for all stakeholders in a flexible and business-friendly manner.

AmCham EU recognises that the Commission's proposal is a key milestone of a lengthy and complex process of reform. As indicated above, the legally required organisational and technological safeguards should be proportional to the risk, cost and current state of technology. We look forward to working with the European institutions to strike the right balance as this process moves forward.

***

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate U.S. investment in Europe totalled €1.7 trillion in 2010 and directly supports more than 4.2 million jobs in Europe.

***

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE TO THE EUROPEAN UNION
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

POSITION STATEMENT

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE TO THE EUROPEAN UNION
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

AmCham EU position on the General Data Protection Regulation

Detailed Analysis of Issues and Recommendations

INFORMATION PAPER

11 July 2012
American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
Email:info@amchameu.eu

Secretariat Point of Contact: Roger Coelho, roger.coelho@amchameu.eu, 32-2-289 10 18

Detailed Analysis of Issues and Recommendations

This Information Paper sets out in detail the position of the American Chamber of Commerce to the European Union (AmCham EU) on the European Commission's proposed General Data Protection Regulation. Together with the Position Paper summarizing the key points, the document incorporates and builds upon our responses to previous Commission consultations on the European Union's approach to the protection of personal information.[1]

Position Summary

The chart below provides a summary of AmCham EU's positions vis à vis data privacy issues outlined in the Commission's proposal. Following the summary table a detailed analysis of our recommendations on the key issues is provided.

Issues	AmCham EU's Position
1. Consent & profiling	AmCham EU believes that rules on consent cannot be "one-size-fits-all". Making explicit consent the norm in every data use scenario will inhibit legitimate practices without providing a clear benefit to data subjects. Instead, AmCham EU encourages the EU to adopt consent requirements that reflect the context in which consent is sought and personal information is used. AmCham EU believes that profiling techniques per se do not need special regulatory treatment given the many safeguards in the draft Regulation. At minimum, the Regulation should make clear that the restrictions on profiling do not extend to beneficial activities such as fraud prevention, service improvement, and marketing/content customization.
2. Definition of personal data	AmCham EU recommends that the context be taken into account in determining whether and when data identifies a data subject. Currently, this important principle is only reflected in a recital. It should be included in the Regulation itself. Incentives should also be provided for companies to make data anonymous or associated with a pseudonym.

[1] See AmCham EU's response to the Commission communication on a comprehensive approach on data protection in the European Union, 14 January 2011; AmCham EU Position Statement on the Commission consultation on protection of personal data', 19 January 2010; and 'AmCham EU response to the Commission consultation on protection of personal data', 19 January 2010, www.amchameu.eu.

3. The right to be forgotten & data portability	AmCham EU agrees that data subjects should have the right to demand deletion of *their own* information, which the data subject has published/posted, and which is reasonably accessible to the controller during the ordinary course of business. Additional obligations on controllers, such as to inform third parties or to delete data created by third parties, threaten to make controllers arbiters of when and what data should be deleted -- a role that they are not in a position to play. AmCham EU supports the right of a user to retrieve, in an efficient and cost-effective manner, any personal information that he or she has made available. To reflect technical realities and allow room for industry innovation, however, the Regulation should explicitly recognize that data cannot always be used "as is" in other services, and the Commission should refrain from standardizing data formats as this would adversely impact innovation.
4. Administrative burden / data controller and processor issues	AmCham EU welcomes the elimination of the notification obligation. But the introduction of a prior authorization or review requirement could delay the launch of new services and hinder Europe's capacity for innovation. More broadly, to encourage responsible behavior, the Regulation should offer incentives to accountable controllers, such as exemption from certain penalties or simplified mechanisms to transfer data. AmCham EU also recommends revisiting the definition of a data controller and joint data controller, and to fine-tune the contractual and liability regime applying to joint controllers to avoid increasing confusion and legal uncertainty in the EU. To enable freedom of contracting and avoid duplicating administrative burdens, AmCham EU also believes that processors should benefit from greater clarity regarding their own obligations. These obligations should be distinct from those of controllers.
5. Fines / Remedies	AmCham EU recognises that meaningful sanctions must be available for flagrant violations that threaten real harm to the individuals affected based on clear rules that ensure a high degree of legal certainty. The sanctions proposed in the Regulation seem excessive, however. Instead, penalties should appropriately reflect the sanctioned conduct. Any fines imposed should reflect when an organisation has sought to behave responsibly.

Detailed Analysis of Issues and Recommendations

6. Delegated Acts / Applicable Law / Governance &Transparency	AmCham EU is concerned that the number and scope of delegated acts in the proposed Regulation creates legal uncertainty, which makes it difficult for businesses to operate and grow. The number of delegated acts should be reduced, and clear timelines should be introduced for those delegated acts that remain. The current criteria for extending the Regulation to non-EU providers are unclear. AmCham EU recommends that only those third country controllers that specifically and intentionally target data subjects in the EU should be subject to the Regulation. AmCham EU strongly supports the principle of a single competent supervisory authority. To promote greater certainty and clarity, the same test for determining an organization's "main establishment" should be applied to controllers and processors and the single supervisory authority's powers should be more clearly specified. The territorial scope of the "one-stop-shop" principle should also be clarified to ensure that data controllers based outside Europe can benefit from it.
7. Certifications and codes of conduct	Certifications and codes of conduct can help organisations to demonstrate their security and privacy commitments and allow for faster adaptation to market developments**.** In AmCham EU's experience, such mechanisms work best when they are industry-driven, and operate at a global level rather than being regional or sector-specific. The Regulation should reflect this.
8. International data transfers	AmCham EU believes that data subjects, controllers and processors would be better served by an accountability-based system that requires data exporters to protect European data regardless of where it is located. If adequacy remains at the centreof the EU's transfer regime, however, then amendments are needed to the proposed rules on standard and contractual clauses, Binding Corporate Rules (BCRs) and derogations to ensure that they enable the efficient transfer of data while providing strong safeguards for personal data. Incentives should be introduced to encourage controllers and processors, where appropriate, to offer additional safeguards.
9. Definition of a child	AmCham EU welcomes the clarity on the threshold age of 13 for obtaining parental consent and believes that the goal of harmonisation should be supported as it improves the current situation of divergent rules in member states.

	AmCham EU also supports notices that are specific to children as a way to increase transparency and user awareness. However, AmCham EU points out the potential ambiguities created by defining a child differently in different contexts.
10. Data breach	In order to avoid data subjects getting "notice fatigue," notifications should be required only where a breach is likely to lead to a significant risk of serious harm to the data subject. A 24-hour notice presumption is unworkable; controllers should be obligated to notify data protection authorities (DPAs) without undue delay.

Detailed Analysis of Issues and Recommendations

1. CONSENT AND PROFILING

A. Consent

Consent -- the ability to make informed decisions about the use of one's personal data -- is an essential element of a robust data protection regime. For consent rules to be workable across all sectors and foster strong data protection, these rules must be clear and balanced. AmCham EU believes:

- **Consent requirements should reflect the context in which consent is sought and personal information is used.** The Regulation currently adopts a "one-size-fits-all" approach, requiring explicit, affirmative consent in all circumstances. This approach -- which fails to distinguish among the many contexts in which data is collected and used, and the different privacy impacts of those uses -- is likely to devalue the principle of consent. This will make it more difficult for individuals to decide when to give consent and when to withhold it. Moreover, prescriptive consent requirements may soon be outpaced by technological change. Explicit consent should be required only where justified by the sensitivity of the data or the risk associated with the particular processing.

- **At a minimum, the impact of requiring that consent always be affirmative and explicit should be further examined before being enacted into law**. Requiring explicit consent will require that a range of common practices will need to be reconsidered and re-architected, imposing potentially significant costs on data controllers, processors and third parties. In marketing, for example, where consent is often the primary basis for data processing, it may make sense to focus less on re-engineering common practices to obtain express consent and more on ensuring that recipients of marketing communications can easily "unsubscribe." The EU should consider the potential effect of the proposed consent requirements, and whether they indeed reflect the priorities of European consumers, before making choices that may impede innovation across the Union.

- **Putting the burden of proof on controllers to demonstrate consent may harm, rather than protect, data subjects. This requirement should be reconsidered.** Many websites will likely require visitors to become registered users in light of the Regulation's reversal of the burden of proof. As a result, these websites may collect *more* information from users than they in fact need. Consideration should also be given to the burden on consumers (for example, extensive tick-box use) which will only lead to confusion - again, this is prevalent in the context of marketing.

- **The concept of significant "imbalance" requires clarification.** This concept could be misinterpreted to prevent controllers from making consent a condition of access to a service. It is also superfluous because the Regulation already requires that consent be "freely given."

- **Organizations should not be obliged to continue offering services once consent is withdrawn**. Withdrawal of consent for processing should be sufficient grounds for terminating service to the data subject.

B. Profiling

Article 20 builds on existing provisions around automated processing, extending them to a potentially broad range of data processing techniques collectively referred to as "profiling." AmCham EU believes that profiling techniques *per se* do not need special regulatory treatment given the many safeguards in the draft Regulation (*e.g.,* the general principles governing lawfulness of processing (Chapter II), transparency and information obligations (Articles 11 and 14) and data security obligations (Chapter IV, Section 2). The approach adopted in the Regulation raises a number of concerns:

- **Article 20 makes no distinction between data processing that identifies an individual and data processing that does not**. As drafted, Article 20 -- which uses the term "natural person" rather than "data subject" -- could be misinterpreted to extend to the processing of a broad range of data *beyond that covered by the Regulation itself*. We assume that this result is not the drafters' intent. But to avoid misinterpretations, AmCham EU recommends using the term "data subject" in Article 20. (This also mirrors the proposed Data Protection Directive; Article 9 of that proposal restricts the profiling obligations to "data subjects").

- **The "significant effect" test is too broad and vague** for wide-spread application given the much broader scope of this Article compared to Article 15 of the existing Directive 95/46. An "adverse effect" test is needed to ensure that the article is not invoked to impede legitimate data processing practices.

- **The legitimate interests of the data controller should provide a legal basis for profiling.** This would ensure that profiling techniques and technologies used to manage, improve, or customise services for similar customers (e.g., for, anti-fraud, accounting purposes, health care purposes under Article 81 etc.) are not prohibited under the Regulation.

- **Article 20 should also be revised to make clear that it does not apply to content customisation.** Profiling and customisation techniques are used in a variety of sectors, ranging from banking to healthcare to retail and serve many legitimate purposes, including monitoring and fraud prevention, service improvements, and marketing. The Regulation should distinguish customisation that is in the individual's interest from profiling that harms or adversely impacts a data subject (e.g., racial profiling). Treating these two activities similarly threatens to impede many valuable consumer-driven services.

2. DEFINITION OF PERSONAL DATA / SECURITY PROCESSING

AmCham EU has consistently advocated for clarity in defining when data is regarded as "personal data," and emphasised that this determination should depend on the context in which the data is processed. While certain recitals and provisions partially address this point, the definitions proposed under Articles 4(1) and 4(2) largely fail to account for the significance of context in determining when data is "personal." In fact, Articles 4(1) and 4(2) expand the definition of personal data to include virtually all data. This expansion is disproportionate and incentivizes controllers to capture more personal data rather than less.

- **Article 4 should explicitly require that context be taken into account to determine whether data identifies a data subject.** Recitals 23 and 24 recognise that context is a relevant factor, and that data which does not identify a data subject is not "personal data." These important limitations should be expressly confirmed in the Article 4 definition of a "data subject". Failure to provide clear and definitive guidance on this point, as reflected in the reasonability test in Article 4.1, may lead to a lack of legal clarity and inconsistent implementation of the Regulation. In particular, the above reasonability test (also reflected in Recital 23) should be made clear that, when a data controller or a third party has no interest in identifying the individual, the data should not be considered personal and the Regulation should not apply.

- **At a minimum, the Regulation should make clear that not all data should be treated equally**. AmCham EU endorses the view, expressed by the UK Information Commissioner's Office in its 27 February 2012 opinion on the Regulation. I It states that it is unrealistic to apply *all* of the requirements of the Regulation to *all* of the many forms of personal data that fall within its scope (and, particularly, to all online identifiers). Instead, context must be relevant in determining what protections are merited. It would be helpful if the Regulation stated this principle explicitly and identified factors that controllers should consider when assessing how the Regulation's rules should apply.

- **The Regulation should expressly recognise the existence of pseudonymous data (i.e. data processed with no consideration of or interest in an individual's identity, which is not apparent to the data controller from the information processed) as a third category of data in addition to personal data and anonymous data.** In addition, Article 10 should explicitly confirm that, where a data controller is unable to identify a natural person from the information processed, the controller is subject only to limited obligations -- specifically those pertaining to security of processing and maintaining documentation. And because data processors may be unable to assess whether the information they hold qualifies as "personal data," AmCham EU recommends extending Article 10 to processors.

- **Anonymization and pseudonymization should be better incentivized.** When personal data is rendered anonymous or pseudonymous immediately

after collection, the provisions of the proposed Regulation should not apply, with the exception of Section 2 relating to security of personal data during the process of anonymization or pseudonymization.

- **AmCham EU recommends that Recital 39, which clarifies that network and information security is a legitimate ground for processing, explicitly identify fraud monitoring and prevention as legitimate purposes. All such processing should be exempt from certain information, access and objection requirements.** The computer security and payment industries process a wide range of data to protect EU citizens and organizations from cyber-threats. This includes personal data theft, identity theft, denials of service, botnets, hacking, spam, phishing, and payment fraud. Requiring these organizations to comply with all of the Regulation's rules, including requirements that data subjects be notified and given access, is neither practical nor appropriate. Recital 39 should be moved to the body of the Regulation, and the Regulation should make clear that information, access and objection obligations do not apply.

- **Recital 139 should require respect for all fundamental rights, including the right to the protection of intellectual property.** Recital 139 correctly states that the right to data protection should be balanced with other fundamental rights. However, it fails to recognise the fundamental right to the protection of intellectual property and trade secrets, which is established in Article 17 of the EU Charter.

- **Genetic data is defined very broadly.** The proposed definition of genetic data would turn inherited characteristics such as hair colour into sensitive data requiring additional protections. A more targeted definition of genetic data should be used.

3. THE RIGHT TO BE FORGOTTEN /DATA PORTABILITY

Right to Be Forgotten

AmCham EU believes that, at the core of the right to be forgotten, is the idea that an individual using a hosting platform should in principle have the ability to delete his or her own data within commercially reasonable limits. However, the right to be forgotten should not mean that an individual can "remove all tracks" from the internet, such as information that was created by a third party. Moreover, the right to be forgotten should be balanced with the right of others to remember. For instance, the recipient of a private message should be entitled to keep a copy of the message he received even though the sender deleted it from his own account.

AmCham EU believes that the draft Regulation's approach to the right to be forgotten has a number of weaknesses, described below:

- **Article 17 confuses the roles of the user, the data subject, and the hosting platform in assigning responsibility for personal data that has**

been made public. Online platforms are not in a position to identify the owners of information published by one of its users, or whether this information would breach privacy. AmCham EU considers that the right to be forgotten should be limited to the user's own information, which the user has posted himself or herself. It should not extend to data posted or generated by third parties (e.g. a user's comment about another user), as these are already subject to existing legal protections *(e.g.*, in case of libel or defamation). In addition, the right should be applied only to data that is reasonably accessible during the ordinary course of business, and data controllers should be able to comply by anonymizing or otherwise de-identifying data.

- **Article 17 fails to reflect business realities.** In situations where an organization and an individual have an on-going relationship that involves the processing of data for multiple purposes, the right to be forgotten may cause disruption. If an individual regularly purchases from an online retailer, for example, the retailer will store and process the individual's personal data both for marketing and account management purposes. If the individual were to exercise the right to be forgotten in an effort to stop marketing messages, Article 17 would appear to require that his or her personal data would have to be deleted, including data held for account management purposes -- an unnecessary inconvenience for both the retailer and individual. The benefit of the right to be forgotten is unclear in scenarios like these, particularly given that Article 19 of the Regulation would provide data subjects with the right to object to processing (including for marketing purposes).

- **It is technically impractical.** In today's online ecosystem, digital data is often replicated across the internet, disclosed in unrelated ways, and stored on servers and platforms that are not under the authority of the data controller. As a result, deletion may not be commercially or even technically feasible. Other provisions of the Regulation already recognize the need for online platforms to provide clear information and control mechanisms to users, including privacy settings that modulate visibility and sharing options. Encouraging users to better utilize these mechanisms is a more workable alternative than an overly broad application of the right to be forgotten.

- **Data controllers may be unable to comply with their obligation to inform third party recipients about individuals who have exercised their right to be forgotten.** While informing third parties may be feasible when a data controller discloses information only to specific recipients, the required notification would be virtually impossible when information is disclosed to an unspecified number of third parties. A data controller's attempt to notify third parties may be further complicated when the information posted by an individual is subsequently altered by the third party. In addition, it is not clear what information needs to be forwarded to third party recipients. AmCham EU proposes to redefine the information requirements in Article 17.2 so that they are proportionate and effective from the outset, limited to those third parties to whom the controller has effectively and knowingly

transferred the information. In accordance with CJEU jurisprudence[i], making information generally available on the Internet does not constitute a transfer under Article 17.2. In particular, certain exemptions should apply, when the identification of all relevant personal data in question proves impossible or involves a disproportionate effort and when in relation to personal data made publicly available by the data subject himself or herself, such right is overridden by the interests or fundamental rights and freedoms of others.

- **Article 17 does not provide for safeguards on member state variation**. The proposal subjects the right to be forgotten to certain exceptions, including where the controller is obligated to retain the information under national law, or where exercise of the right would interfere with free expression. However, the Regulation does not harmonise these and other national laws. As a result, there may be substantial variations in the application of the right across member states.

- **The right to be forgotten does not define clearly how it relates to the exercise of other fundamental rights** such as the rights to information and freedom of expression. AmCham EU recommends that the Regulation include a broad definition of "journalistic purposes" in the articles -- as opposed to the recitals -- to better protect the important fundamental rights of freedom of expression and information.

- **The right to be forgotten causes particular issues in the health care sector.** While there are exemptions from the right to be forgotten in the area of public health (Article 81) and scientific research (Article 83), it is not clear when and how such exemptions apply. The application of such a right could potentially invalidate scientific findings in clinical trials, epidemiological studies and medical research.

Data Portability

AmCham EU supports the right of users to meaningfully control their data, including the ability to retrieve their data in an efficient and cost-effective way. However, any rules on data portability must account for technical realities. Services that use personal data vary greatly in the types of data they use, and the way in which that data is integrated into other services. Cloud computing services reinforce this complexity, as different sources of data are combined and processed for innovative purposes. This competitive differentiation is key in cloud computing, particularly in the enterprise space.

While users can legitimately expect to control their data, transferring information such as comments, group photos, or connections is considerably more complicated than, for instance, transferring a telephone number. Standardizing the format of data transfers -- which the Regulation empowers the Commission to do through delegated acts -- will not address this complexity and may actually hinder innovation. As a result, AmCham EU recommends:

- **References to standardization through delegated acts should be deleted**. In addition, the right to portability of data should explicitly recognize that data cannot necessarily be used "as is" across services, and that the controller or processor may choose the format in which data is transferred, consistent with technical requirements of the transfer and the solution.

- **The right should be limited to data that the user posts himself or herself.** Technical data that is generated by the controller in the provision of a service should not be subject to the right of data portability.

4. ADMINISTRATIVE BURDEN / ROLES OF DATA CONTROLLERS AND PROCESSORS

Reducing the administrative burden on controllers and processors and enabling a single market for data in the EU are among the primary objectives of reforming the EU's data protection framework. These are worthy ambitions, and eliminating the notification system is a positive step towards achieving this goal. Care needs to be taken, however, to ensure that the Regulation does not replace existing burdens with new, heavier ones.

- **The obligations set out in Articles 33 and 34, involving privacy impact assessments and prior authorization, should be reconsidered.** While the Regulation eliminates the requirement to notify Data Protection Authorities (DPAs), companies are expected to keep even more detailed records in-house and are expected to conduct a privacy impact assessment and obtain prior clearance for a wide range of processing operations such as processing of health data. Requiring prior clearance undermines the ethos of the revision, which was intended to instill a culture of accountability backed by *ex-post* oversight rather than perpetuate *ex-ante* 'box-ticking.' Requiring prior consultation could lead to a backlog of work for already-overburdened DPAs and could delay the launch of new services, impeding innovation and medical research including the introduction of new treatments.

- **The Regulation should offer clear incentives to accountable controllers**. Directive 95/46 provided incentives to appoint Data Protection Officers (DPOs), via a simplification or waiver of notification requirements. The proposed Regulation lacks similar incentives for companies to act responsibly. Accountable controllers could, for example, enjoy less prescriptive requirements or benefit from simplified mechanisms to transfer data. The Regulation could also allow companies to appoint regional DPOs.

- **The "data controller" should be re-defined as the entity which determines the "purposes" of the processing**. Otherwise, any service provider with a certain level of sophistication will qualify as a joint controller because it determines part of the means and conditions of the processing. This would only reinforce the existing confusion around the concepts of data controllers and joint controllers. In addition, joint controllers should be allowed to contractually allocate their respective liabilities between themselves and vis-à-vis data subjects (Article 24) to reflect their effective processing roles and their relationship with data

subjects. Otherwise, the risk of absolute and indiscriminate joint liability is likely to deter many economic operators from doing business in Europe.

- **Article 82 provides an empowerment for Member States to adopt specific laws for processing of personal data in the employment context.** We assume the intent of the legislator is to provide flexibility for Member States to glue the new Regulation into their legal systems, and not to provide an option for Member States to adopt local regimes. In order to avoid misinterpretation, we recommend robust clarification of Article 82.

- **Processors have limited and distinct obligations that do not simply mirror those of controllers.** While a recital in the Regulation recognises that the responsibility and liability of controllers and processors should be clearly apportioned, the articles lack clear guidance on the rights and responsibilities of processors and controllers. While greater clarity is warranted in the apportionment of responsibilities, we believe that they should be appropriately embodied in the contracts between controllers and processors. Independent obligations upon processors will create needless uncertainty in the controller processor relationship – as processors will need to independently evaluate their obligations vis-à-vis controller instructions. Furthermore if processors have separate obligations they will need to take greater steps to know about the data they are processing, not just relying on controller representations and instructions again confusing the relationship and also contravening the principle of data minimization. This is not in the interest of data subjects, unnecessarily restrict contractual freedoms, duplicate administrative burdens, and lead to inefficiencies in enforcement. It makes little sense, for example, for data processors and data controllers to document the same process twice. Moreover, in the cloud context, requirements such as obtaining prior authorization from the controller for the processor to enlist sub-processors (Article 26(2) (d)), especially if interpreted to require prior authorization to use specific sub-processors, impose burdens with no clear benefit in terms of enhanced data protection. This requirement should be removed or be clarified to permit general consent to use sub-processors.

- **Privacy by Design and by Default[2] (PbD) are separate concepts, the impacts of which need to be clearly understood. As such these concepts, if included in the proposal for a Regulation, should offer industry the flexibility to propose and implement details that are appropriate for their users.** Organizations should integrate privacy considerations into their internal processes, but the actual way they do so should leave room for adaptation based on their business models, size and interaction with personal data. It is essential that any PbD concept not introduce specific technology or operational mandates. Provisions on "Privacy by Default" inevitably raise more questions than they answer. In practice, products and services can be very sophisticated and it may be unclear what the most appropriate default privacy setting should be in specific instances.

[2] Note that AmCham EU issued an opinion on Privacy by Design, 2 November 2011.

- **The Regulation should provide for a minimum phase-in period of five years before it applies to data processing that is ongoing when the Regulation enters into force.** Bringing all such processing into compliance with the Regulation will require *tens of thousands* of agreements to be revisited. A five-year phase-in period will give data controllers and their partners the time needed to achieve compliance.

5. FINES / REMEDIES

Data protection obligations are only effective to the extent they are enforced. Consistent with this view, the Regulation includes strong sanctions for violations. Less helpfully, however, the Regulation's rules could prevent DPAs from considering the facts of a case, and instead require them to apply the same sanction penalties to intentional and negligent violations, regardless of their severity or impact. As a result, a company that negligently fails to use an electronic format for access may face the same penalty as a company that repeatedly and intentionally processes data without providing notice. To ensure that sanctions are proportionate and fair, AmCham EU believes that:

- **DPAs should consider the circumstances of each violation, imposing maximum penalties only where truly warranted.** As drafted, the Regulation restricts DPAs' discretion by requiring -- instead of enabling -- them to impose penalties, even when the violation may not merit sanctions or when an informal response is sufficient (*e.g.,* warning letters).

- **Fines should be subject to a cap.** Applying the calculations in the proposed Regulation, the level of penalties can, for some companies, result in administrative fines of hundreds of millions of Euros. AmCham EU recommends that each range be subject to an annual cap -- specifically 0,5% of annual worldwide turnover up to 500,000 EUR, 1% up to 1 million EUR, and 2% up to 2 million EUR.

- **In assessing fines, DPAs should be required to consider an organization's cumulative efforts to behave responsibly, consistent with the Regulation's responsibility principle.** For example, if an organization implements reasonable security measures but a data breach occurs anyway, the fine should reflect this.

- **The Regulation should make clear that sanctions can only be imposed by the competent DPA based on the one-stop-shop model.** The Regulation is ambiguous regarding the application of the one-stop-shop model to sanctions.

- **The Regulation should require that fines account for whether an individual or entity has been subject to sanctions in another proceeding for the same conduct.** A party should not be penalized twice for the same conduct. The rules on collective redress also merit reconsideration. The proposed Regulation would allow consumer organizations or claim foundations to bundle claims of data subjects and initiate a collective redress

action. The potential scale of such collective actions, in terms of time, cost, and outcome -- on top of administrative penalties -- could expose companies to significant and disproportionate financial liabilities.

- **Sanctions should be based on the harm caused, and not on the size of the organisation.** In this vein, it is puzzling that the Regulation foresees an exemption for SMEs. Similarly, in assessing fines, careful attention should be paid to the damage inflicted to ensure that penalties imposed are proportionate to harm.

6. DELEGATED ACTS / APPLICABLE LAW / GOVERNANCE / TRANSPARENCY

AmCham EU has consistently advocated for clear data protection rules that apply to businesses operating in Europe. As a result, we welcome the proposal's efforts to create one set of rules that is applicable in all member states. However, the proposal introduces new uncertainties by providing for numerous delegated and implementing acts, unclear rules on the scope of applicable laws, and a lack of transparency with regard to the European Data Protection Board. AmCham EU would welcome additional clarity in these areas.

A. Delegated Acts

The Regulation relies on delegated acts in 26 specific points (and 19 on implementing acts). These delegated acts specify the conditions, criteria, and requirements of many of the most important obligations imposed on businesses. In light of their reach and importance, greater certainty is essential so that organisations can understand what is required for compliance. AmCham EU recommends that:

- **Delegated act provisions that deal with essential elements of the law should be deleted.** Essential elements of the Regulation -- including (i) the material scope of the Regulation and the lawfulness of processing (Article 6(1)(f)), (ii) breach notification (Articles 31 and 32), and (iii) administrative sanctions (Article 79) –should not be subject to delegated acts. These rules should be set out in the Regulation itself. Establishing these essential elements through delegated acts reduces legal certainty, making it difficult for controllers and processors to comply and confusing data subjects and authorities.

- **Delegated acts that threaten technology neutrality should also be deleted.** Many of the proposed delegated act provisions enable the Commission to replace industry innovation with regulatory intervention by adopting prescriptive rules, standards, and formats. These Commission rules might prefer certain solutions over others, undermining incentives to invest in more privacy-friendly technologies that depart from prescribed solutions. Provisions that allow the Commission to "specify the electronic format and the technical standards" should be deleted (*e.g.*, relating to data portability, privacy impact assessments (Article 33), prior authorization for processing

(Article 34), privacy by design and by default, and privacy impact assessments).

- **Some delegated acts undermine predictability and/or business certainty: a clear timetable should be set for the adoption of those delegated acts.** While the proposal anticipates that a number of issues will be dealt with via delegated acts, it fails to set out a timetable for the adoption of such acts. As a result, businesses could face a lengthy period of uncertainty about their obligations and rights. The Article 29 WP has acknowledged this concern, and has called on the Commission to "*set out which delegated acts it intends to adopt in the short, medium and long term*."[3] AmCham EU recommends that the Commission submit legislative proposals by a deadline specified in the Regulation.

B. Territorial Scope & Applicable Law

AmCham EU supports the objective of ensuring an appropriate level of data protection to all data subjects in the EU. We also and appreciate efforts to minimize burdens on organizations not established in the EU who do only occasional business with EU data subjects (*e.g.,* Article 25 paragraph 2 (d)). However, the Regulation must more clearly explain when non-EU controllers are subject to EU law. Specifically, AmCham EU recommends:

- **Profiling should not be a criterion for the extension of the territorial scope of the Regulation.** The Regulation applies to non-EU controllers when their processing activities relate to "monitoring the behavior" of individuals. It is unclear whether "monitoring" would capture profiling. If profiling is captured, we question whether this constitutes an adequate nexus to subject controllers to EU jurisdiction. Moreover, there may be little that European DPAs can do to enforce the Regulation against non-EU data controllers. The Regulation should not lead EU consumers to believe that the law offers them a degree of protection that it cannot deliver.

- **Article 3 should be limited to those third country controllers who specifically and intentionally target individuals residing in the EU.** The Regulation also applies to non-EU controllers that "offer goods and services to EU residents." The fact that a third-country e-commerce website can be accessed and viewed by individuals in the EU should not in itself be considered "offering of goods and services to EU residents." Likewise, the use of general web analytics, used by the operators of websites around the globe that may be visited by individuals from the EU, should not be deemed to constitute monitoring of EU residents' behavior. Instead, concrete criteria – such as offering shipping to EU member states – should be considered.

[3] *See* Article 29 Working Party Opinion 01/2012, 23 March 2012, p. 7.

C. The "one-stop shop"

AmCham EU welcomes the principle of a single competent supervisory authority. To ensure that the framework will yield the anticipated benefits for businesses in terms of reduced administrative burdens and simplified compliance, however, the single DPA mechanism must be fully integrated throughout the Regulation.

- **Key provisions in the Regulation should be more clearly subject to the single supervisory authority concept**, including the rights of data subjects and their associations to lodge complaints with any supervisory authority (Article 73), the supervisory authorities' duty to hear and investigate such complaints (Article 52), data subjects' rights to bring proceedings before the courts of their place of residence (Article 75), and supervisory authorities' rights to take provisional measures against controllers established in other member states (Articles 55 and 56). Because these provisions do not explicitly recognize the primacy of the competent supervisory authority, it is unclear to what extent the enforcement of the Regulation vis-à-vis a given controller will rest with that authority. Furthermore the application of the controller concept to the enterprise as a whole should be possible to truly create a "one-stop-shop". In addition, Chapter VII (co-operation and consistency) should explicitly require DPAs to refer complaints and investigations relating to a controller to that controller's competent supervisory authority.

- **As a matter of consistency, the definition of "main establishment" (Article 4(13)) should not be different for controllers and processors.** Indeed, depending on the context, any organization may be a controller in certain cases and a processor in others. As drafted, the Regulation would subject such organizations to potentially different supervisory authorities -- depriving them of the benefit of the one-stop-shop.

- **Controllers and processors should determine the location of their main establishment based on a list of possible factors, and then communicate this to the competent supervisory authority.** This would provide legal certainty to the controller or processor about the location of its main establishment and the identity of its single supervisory authority.

- **Joint controllers -- whether belonging to the same group of enterprises or not -- should be entitled, but not required, to designate one competent authority to monitor their joint data processing activities.** This should be the authority most closely connected to the processing.

- **Finally, where the same processing of personal data takes place in the context of the activities of an establishment of a controller in the Union and the activities of a controller within the same corporate group not established in the Union, the EU based controller should be responsible for EU data protection compliance in respect to the data processing activities taking place within that corporate group.** Otherwise, if Articles 3(1) and 3(2) were to be applied cumulatively, the rules concerning the competent data protection supervisory authority would be seriously

compromised. If there is already an EU based controller within a corporate group, that controller should be responsible for compliance in respect of the relevant data processing (as per Article 3(1)).

D. The European Data Protection Board

AmCham EU welcomes the creation of the European Data Protection Board (EDPB). In light of the Board's many important roles, however, transparency and collaboration between the Board and all stakeholders is imperative.

- **There is no need for *all* discussions of the Board to be confidential (Article 72).** While we understand the need to maintain the confidentiality of documents and proceedings relating to specific cases, extending confidentiality to general debates and decisions is unjustified. As a public institution, the EDPB should be fully accountable and subject to the same freedom-of-information obligations as other EU institutions.

- **AmCham EU also recommends the creation of a consultation and decision-making mechanism for the Board in which all interested stakeholders, including industry, can participate.** We look to the EDPB as a facilitator of open and transparent cooperation between businesses and supervisory authorities, which will enhance the protection of personal data and privacy. In this spirit, the EDPB should be obliged to openly consult all interested stakeholders before publishing opinions and decisions.

- **The consistency mechanism is welcomed in principle, but its proposed implementation must be improved**. In particular, the process must be completed within clear and short time-limits (i.e., a maximum of four months for the overall process) and be actionable by the data controller itself in order to be compatible with the realities of commerce and trade. As proposed, the consistency process could take over 15 months, hampering commerce and innovation in the Union.

7. CERTIFICATION / CODES OF CONDUCT

The Regulation helpfully promises to promote certification mechanisms that encourage organisations to demonstrate their data privacy and security commitments. AmCham EU welcomes such efforts, and believes that industry-driven certification mechanisms and data protection seals and marks developed and managed by industry should be favored, and should remain voluntary and affordable.

- **Certification mechanisms should be open to companies both inside and outside the EU.** The Regulation should promote *international* certifications -- including EU-adopted international certifications -- rather than sector-specific or regional certification programs, which can lead to fragmentation of data privacy and security standards. And all relevant stakeholders, including the Commission, should be involved in providing technical

expertise to develop mechanisms that maximize consumer protection while establishing realistic standards.

- **These mechanisms should be industry-driven.** Industry is able to adapt to new market realities at a faster pace than government, and is incentivized to enforce proper use of certifications. Public authorities can provide incentives to participate, clarify predictable procedures for the adoption of opinions or findings, and ensure that codes of conduct support EU-level objectives (as opposed to the current situation, where a European-level body is charged with assessing a European-level code against a series of national tests).

- **Certification mechanisms should also spur innovative solutions for consumers.** For example, certifications could be made available for those enterprises that go beyond the obligations in EU law, such as for controllers or processors who offer additional measures to protect transferred data that go beyond those set out in the Regulation's safeguards.

- **The Regulation should not only permit codes of conduct -- it should support them.** Codes of conduct can "future-proof" legislation by allowing it to remain technology- and business model-neutral. Moreover, codes of conduct can generally be developed faster than legislation and can support additional objectives, such as consumer protection, that do not map to current legislation. Codes of conduct also obviate the need for many delegated acts.

8. INTERNATIONAL DATA TRANSFERS

Because new rules that enable secure, simplified data transfers are essential to European competitiveness, AmCham EU welcomes many of the proposed reforms relating to data transfers to third countries -- including the confirmation that BCRs are available to processors and require approval from only a single supervisory authority, the fact that transfers pursuant to an approved BCR or standard data protection clauses no longer require prior authorization, the recognised need for international cooperation, and the inclusion of "legitimate interest" as a derogation to the transfer prohibition. However, despite these improvements, problems persist. For example, there is no single solution for global transfer activities, such as those involved in cloud computing.

- **AmCham EU favours an accountability-based system that requires data exporters to protect data or face sanctions for non-compliance.** The proposed Regulation falls short of its goal to replace burdensome *ex ante* obligations with *ex post* requirements to protect data. An accountability-based data transfer regime in contrast, would be in line with the principle of self-regulation reflected in other parts of the Regulation, such as the codes of conduct provisions. Companies that invest in comprehensive privacy policies, procedures, and standards consistent with industry best practices should be allowed to process personal data freely across borders.

Detailed Analysis of Issues and Recommendations

- **If adequacy remains at the core of the regime, the Regulation should streamline the process underpinning an adequacy assessment.** The current adequacy procedure is underutilized because it is excessively complex and burdensome. Article 41, which lists the criteria under which the Commission may make an adequacy determination, should provide for a simplified assessment.

- **The Regulation should also make clear that derogations enabling transfers apply even where a country or sector has been found inadequate.** Although Article 41(6) of the proposed Regulation provides that the prohibition on transfers of personal data in case of inadequacy is "*without prejudice to Articles 42 to 44,*" Articles 42(1) and 44(1) suggest that safeguards and derogations enabling transfer apply *only* if the Commission has not taken any decision on adequacy. The text should clarify that safeguards and derogations, such as the standard data protection clauses, apply when the Commission has found the destination otherwise inadequate.

- **AmCham EU welcomes the new rules on standard data protection clauses but believes that reforms are needed to make these important tools easier to use and more effective**. Standard data protection clauses are critical for enabling the safe transfer of data across borders. We welcome the decision to not require prior authorization for transfers based on standard clauses. To further facilitate the use of standard clauses, Article 42(3) should be revised to make it clear that no additional administrative requirements (such as notification, for example) may be imposed where a data exporter relies upon approved standard clauses. In addition, in order to better adapt the usage of standard clauses to the cloud environment, supervisory authorities should recognize (possibly via a certification) those cloud providers that offer additional legally binding safeguards over and above the standard data protection clauses.

- **AmCham EU welcomes the extension of BCRs to processors, and the proposed improvements to the BCR process. But the requirement that BCRs be "legally binding and apply to and are enforced by every member within the (…) group of undertakings" (Article 43(1)) is too broad.** Multinationals should be free to include only certain subsidiaries in their BCRs, depending on their needs and in keeping with the flexibility that BCRs are meant to provide.

- **While we also welcome the addition of a derogation based on "legitimate interest," the conditions imposed on the derogation are too onerous to make it useful.** For example, by prohibiting transfers that are "frequent or massive," the derogation is unlikely to benefit providers of cloud services. "Massive" is an undefined and unclear standard, and likely to become less relevant over time. For this reason, AmCham EU believes that organisations should be given the ability to define appropriate safeguards including for transfers that are "frequent or massive". Further, the obligation to inform the supervisory authority about a transfer creates red tape while providing no clear benefit to data subjects. Consistent with the accountability principle, a data exporter should be entitled to rely on its legitimate interest

to transfer data where it can justify and document its position when required as part of an *ex post* review. Even if this accountability structure is not adopted, the Regulation should clarify that the derogation based on "legitimate interest" covers data transfers to public authorities in other countries that are necessary for the data controller or processor to comply with that country's laws, or legal proceedings (such as e-discovery), including laws aimed at preventing money laundering or terrorism.

- **The Regulation should expressly include the EU-U.S. Safe Harbor program as an appropriate safeguard enabling data transfers.** Although AmCham EU understands that the Safe Harbor remains in place under the proposed Regulation, explicitly referencing this mechanism in an article or recital will avoid confusion.

9. DEFINITION OF A "CHILD"

The opportunities that the internet create for children must not be ignored and it is important for regulators to find the right balance in order to preserve the huge benefits that children are getting from the online environment and at the same time keep them safe from possible risks.

AmCham EU believes that the appropriate level of regulation should be determined in accordance with the actual level of risk and the ability of the data subject to understand the consequences of his/her actions in the online environment depending on the circumstances, means and purpose of collection and processing.

AmCham EU makes following recommendations:

- **There is a need to recognize that as technology enables more widespread data collection from children**, rules should evolve to protect children's privacy and safety online while at the same time preserving the educational and social benefits of increased interactivity.

- **Meaningful parental consent, proportional to the type and proposed use of the data**, is critical to achieving this balance.

- **Clarity on the threshold age of 13 for obtaining parental consent is welcomed**. Same, the goal of harmonization, as it improves the current situation of divergent rules in member states, is supported as well as the proposal to craft notices that are specific to children and written in appropriate voice in order to increase transparency and user awareness.

- **Further discussion and clarification** of the limitations on performing profiling activities in relation to children under 13 is welcomed.

- **There is ambiguity created by defining a child as under 18 in contexts other than obtaining parental consent**. For example, the current proposal

creates an obligation to perform privacy impact assessments (PIAs) for all processing involving children under 18. This should be clarified so that not all processing of data from users under 18 should trigger PIA. Instead, the appropriate trigger should be determined by the actual level of risk to the data subject. Similar clarifications are required with regard to the right to be forgotten (which applies "especially" where data was collected when the data subject was under 18).

10. DATA BREACH

Breach notice obligations encourage data controllers to manage personal data more securely, and foster confidence in third-party data processing. However, not all breaches threaten user privacy. In order for the EU's regime to be workable, AmCham EU recommends that it focus on data breaches that are likely to have serious and negative consequences, rather than on *all* breaches.

- **Controllers should be required to notify both DPAs and data subjects only where a breach is likely to lead to significant risk of substantial harm to the data subject**. The proposed Regulation -- which requires that DPAs be notified of *all* breaches regardless of size or severity -- will overwhelm DPAs. Lacking resources to deal with these notifications, DPAs may miss important data breaches. This is recognized in Recital 67 of the draft Regulation, but is not clearly addressed in Articles 31 and 32.

- **The usability of the data and the circumstances in which the data was lost should also be considered in determining whether notification is needed.** If data has been effectively rendered unintelligible, for example by encryption or equivalent means, notification obligations should be alleviated or waived. This pragmatic approach, which the Regulation already applies to notification of data subjects (Article 32), should be extended to DPA notifications (Article 31). Similarly, if data was accidentally destroyed or was lost inadvertently (i.e., no one hacked into the system where the information resided, or stole physical data), those facts in the context of an event should bear on the likelihood that the data has fallen into the hands of an unauthorized person whose possession of the data gives rise to the risk of harm.

- **The 24-hour presumption for notification of personal data breaches is both impractical and counterproductive.** In practice, depending on the nature and scope of a personal data breach, the data controller will require more time to understand the nature of the breach, who is affected, and whether the breach poses a substantial likelihood of harm to the data subjects involved. It would be premature to notify a personal data breach before these essential facts are known and understood, and may both jeopardise an investigation, and unduly distress data subjects who may not be exposed to any tangible harm or who are unable to take steps to protect themselves until more information is known. Moreover, the priority should be to investigate a breach and take appropriate action to limit loss or damage.

Detailed Analysis of Issues and Recommendations

- **Based on the experience of the ePrivacy Directive breach notification, it is crucial to ensure that the Regulation harmonises implementation across member states**. This harmonisation should extend to processes (*e.g.,* a designated competent authority) and formats (*e.g.,* standardized notice forms and a single point of contact). This process should be as simple and efficient as possible, given the limited time frame for notifications.

- **The breach notification provisions should also reflect the fact that not all data controllers have a direct relationship with or can even identify the end user**. In some contexts (*e.g.,* B2B), providers are typically at least one step removed from the end users of the service and may lack the capability to identify end-users (who may be employees of enterprise customers, end-users of wholesale customers etc.). In these cases, providers should only be required to notify the downstream customers. The provider with the final retail relationship should be the one obligated to notify their end user of any breach.

***

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate U.S. investment in Europe totalled €1.7 trillion in 2010 and directly supports more than 4.2 million jobs in Europe.

***

[i] in the *Lindqvist* case (Case C-101/01)