Trans-Atlantic Business Council:
General Considerations on the EU Draft General Data Protection Regulation

The Trans-Atlantic Business Council (TABC) would like to recognize the significant work that the Parliament, Council and Commission have done on the Draft General Data Protection Regulation (GDPR). We also appreciate the number of forums, workshops and meetings that have been held to provide the opportunity for all stakeholders to comment on the draft. We have tried to also meet the requests from the various drafters to provide specific, and where possible consensus, comments on the text that address the concerns of business on the potential negative implications on some aspects of the draft to EU innovation and economic growth.

The explosion of proposed amendments has made the development of specific comments more problematic and less potentially useful. In reviewing the history of business comments into this process, we recognize that while there are numerous particular issues that business have commented on there are some issues and themes which have been constant throughout the process. Rather than focusing on the potential issues that each amendment may create, we are focusing these comments on the guidance business believes is essential to achieve a privacy compliant ecosystem that continues to enables business to seize the potential opportunities the Internet presents for economic and societal benefit.

Focus on the Issues

Since the GDPR has been under consideration, issues related to lawful access to information through national security services have arisen. These issues are global in nature and remit and raise legitimate concerns across stakeholders as to the nature, scope and oversight of such programs and access. Obligations related to national security access which can preclude disclosure of the request for information may conflict with other possible obligations related to personal information, especially obligations of privacy/data protection. While business may be the custodian of such information either directly from the data subject or for another business which provides services to the data subject, they are not in a position to judge the merits of either the request or the program. Businesses must comply with laws that exist in the jurisdictions in which they provide their services. Thus inherent conflicts of laws may exist between obligation to protect data and obligations to disclose data pursuant to national security obligations. The US/EU Safe Harbour in its current form does not apply to national security access requests to personal information. Issues of the sufficiency of the programs or the appropriateness of the requests for access cannot be determined by business and are the purview of inter-governmental consultation. These issues go beyond appropriate collection, protection and use limitations of information in the context of providing commercial services. We urge all governments concerned to continue to engage in constructive dialog to address outstanding issues, provide appropriate assurances and develop agreements on processes and procedures so that business may both engage in commerce and comply with legal obligations of all types with greater certainty and predictability. Furthermore, this dialogue and the subsequent results are welcomed by industry as a necessary measure to restore trust into data driven business models.

GDPR Objectives and Potential Improvements

We are supportive of the general objectives of the draft regulation which include enhancing privacy protection and user trust while lowering administrative burdens and complexity for business. We also believe that greater legal certainty and consistency in the process and outcomes will benefit both users and business alike. These collective themes are part of what we believe to be an opportunity to optimize the legislation to provide the needed protection of data subjects while enabling business to develop new and innovative services that enhance economic growth and EU competiveness.

In the main, our comments are addressed to areas where the method chosen to implement the broadly agreed objectives may either create needless burdens or unintended consequences. This results in a zero sum game where opportunities are needlessly forgone and sub-optimal solutions result. Some comments also go to a concern of interpretation due to lack of clarity or specificity in the drafting which undermine the enhanced legal certainty that is often considered one of the great benefits of a regulation. On this last issue, we wish to be clear in our intent and meaning. A request for more specifics is not a request for top-down, detailed and proscriptive rules – nothing would stifle innovation faster than that. Our request for specificity is to have enough information and context provided so that we may appropriately evaluate the potential impact of the draft on business models and operations. This uncertainty is magnified where concepts are subject to delegated or implementing acts and the current consistency mechanism.

One potential area of improvement which is considered but may be lacking in execution is the ability to apply the regulation in context. Privacy, while a fundamental right, needs to be applied in varying contexts. Privacy principles can apply fairly easily across contexts but the detail of a regulation needs to consider context in application; one size does not fit all. Using information on a business card in a B2B context is different than collecting consumer information in a transaction, for example. The range and scope of collection and use of information varies significantly across contexts creating different considerations of what is appropriate and proportionate in context. We are concerned that despite the best efforts of the drafters to address such needs in the GDPR they have come up short. The GDPR could benefit from a more risk-based approach in the drafting which would help provide guidance and flexibility to address many of these context issues.

Below, we provide a list of the main issues that we believe could create undue burdens for business or unintended consequences which would ultimately, risk undermining the attractiveness of the European Union as a destination for jobs-creating investment and innovation. The topics outlined in this document represent a consensus across many businesses on both sides of the Atlantic of some of the most problematic aspects of the GDPR that we urge Parliament, Council and the Commission to maintain as objectives and desired outcomes as it undergoes further review.

Changes to Lead Authority: We welcomed the provision in the original draft GDPR that provided for the establishment of a lead Data Protection Authority (DPA) located in the country of a business' main establishment as a vast improvement over the fragmentary jurisdiction provided by the current Directive. Thus, we regard any amendment that limits the lead DPA role to a more minimal *point of contact as* a step backwards. This likely would result in added expense and likely confusion for many companies that would be required to deal with DPAs from multiple

jurisdictions, and ultimately decrease the attractiveness of investment or increased business presence in the EU. We believe that a more appropriate solution to address cooperation among DPAs and assurance that the Data Subject is also appropriately represented would be for the Lead Authority to continue to be the only authority that the business must deal with and to act as the investigatory authority, but, where an individual has lodged a complaint with their Data Protection Authority, to add a role for that Authority to cooperate with the Lead Authority in the resolution of the issue.

Legal Basis for Data Processing/Legitimate Interest: While we appreciate the concerns that an overbroad interpretation of Legal Basis could lead to abuse, proposed restrictions on the topic needlessly constrain the essential flexibility that the concept provides to allow the legal instrument (Directive or Regulation) to be adapted to changing technologies and circumstances. We are also mindful of the fact that the EDPS and other Authorities have cautioned us time and again not to be too narrowly focused on consent as it is only one means amongst others under the law to process information. Our concern is that the proposed amendments on legal basis and other topics force consent to be the principal basis for processing which would create significant burdens and result in untended consequences that may diminish the potential benefits to individuals inherent in the technologies and business models by introducing needless delays and interrupting services to obtain new variants of consent.

The combined impacts of proposed amendments aimed at tightening the consent requirements and restricting the processing of personal data based on legitimate interest will, at minimum, hamper basic customer service functions, and more broadly, impede the use of analytics in a way that benefits the greater good.

- Concerning the former, for example within the service of issuing and managing a credit card, a bank must process its customers' personal data to prevent fraudulent activity with the credit card in question. When the data subject withdraws its consent to such processing, the bank should not be obliged to continue to offer the service of a credit card. The service in this case cannot be performed at the appropriate standard of quality and efficiency; moreover, since the prevention of credit card related fraudulent activity requires the processing of personal data not only of the credit card owner but also of an as wide as possible sample of the bank's customers in order to establish patterns of activity and detect fraud through the deviation of such patterns, the detriment from the withdrawal of consent will affect a wide and undeterminable number of the bank's customers.
- The amendment clarifying that the "legitimate interests" exemption only applies in "exceptional circumstances," would impose time-consuming and costly demands on companies to comply with additional requirements, and pose uncertainty and practical problems such as how to properly evaluate others' legitimate interests and provide information about why their own legitimate interest should prevail. Also important, it creates uncertainty about the "legitimate interest" of processing personal data in an employment context.
- Also concerning to us is language in some amendments addressing situations where the "legitimate interests" of a controller would not prevail if the processing involved sensitive data, location data, and biometric data or included profiling and large scale data combinations. Such restrictions would hamper the use of analytics for important health- and safety-related research or other research and/or functions aimed at serving a company's workforce or benefiting the population in general.

Broader Scope of Personal Data: We note that the Report expands the scope of controls and definition of personal data. This expansion raises many of the same concerns as the constraint on legitimate interest. IP addresses, for example, are now more clearly included in the definition of personal data. IP addresses are not always static and identify devices rather than people; they are part of the inherent functioning and connectivity of the Internet as well as essential elements in virus checking and adaptive access control mechanisms. All of these applications of IP addresses are part of needed information to fulfil customer requests and enable many business functions. Subjecting IP addresses to consent requirements would unduly hamper operation of the Internet and functionally hollow many of these security applications. This is just an example of the potential negative consequences that can result from the proposed expansion in definitions and scope of application.

Profiling: The Report includes amendments that define profiling in a way that greatly limits its use in every context and ultimately works against the interests of EU-based companies or individuals. It should be recognized that most companies use profiling to evaluate and analyse data and use such data proactively for legitimate business purposes, including identify verification and fraud detection and prevention. The amendment has the impact of effectively "demonizing" profiling technology per se, rather than aiming to limit actual or potential negative uses of this technology whilst still protecting beneficial uses. In addition, it does not take into account the fact that there are different levels of risk associated with profiling and disparate types of impact on the privacy of individuals also related to the sensitivity of the data processed with profiling. In sum, a one-size-fits-all approach is not appropriate.

- We propose that the prohibition should focus on the negative uses of profiling techniques which are either "unfair" or "discriminatory" rather than the technology itself; this would also be in line with the technology neutrality principle of Recital 13.

Roles and Responsibilities of Controllers and Processors: The current Directive defines the relationship between a data controller and a data processor working on their behalf by clearly demarcating their roles and liabilities. The controller remains responsible to the data subject for the protection of the data subject's rights. The processor's main obligation is to securely protect the data they are instructed to process. The controller defines the conditions within which the data processor should work and passes on those obligations to the processor contractually, according to the level of risk involved with each particular processing.

The draft regulation would fundamentally change this concept – and inject confusion into well-settled contractual relations -- by establishing joint liability between all data controllers and data processors. where obligations are directly imposed on the processor by law (as opposed to by contract with a controller) the processor can no longer rely on the controller's instructions alone, and will thus have a need to "know" the data subject and the context of the data processing in which they are involved in order to understand their obligations to secure the data. Conversely though, because the controller is no longer fully and exclusively in charge of com-plying with the legal requirements on processing, its own ability to properly assess, understand and manage the risk involved in the processing is damaged. Last but not least, the risk to the privacy of the data subject is also increased, both because documentation and information requirements are duplicated in breach of the data minimization principle, and because the data subject loses the certainty of having to deal with one single entity, the data controller, when seeking remedy. This blurring of lines between the two parties' roles in every case, without consideration of the context or risk, creates unnecessary compliance burdens, impinges on companies' freedom to contract, and is likely to confuse established consumer relationships.

Documentation: Business has highlighted the concern that the level of documentation has not been specified in the original draft. In that draft, documentation was specified at the level of a "processing operation" which was not further defined. Our understanding is that the drafters are attempting to limit the documentation requirements in principle, but the combination of concepts related to documentation that needs to be maintained and information that needs to be provided to data subjects has led to greater confusion. Business would request that a clearer delineation of the nature and detail of documentation be provided, with the GDPR focused on the former. Overly detailed documentation requirements would result in needless administrative burdens and requirements to publish information related to security or commercially sensitive information could significantly undermine the ability to conduct business in the EU.

Cross Border Data Flows: European and global companies have a substantial economic need for cross-border data flows between countries and regions with very different privacy regimes. Facilitating responsible global information flows is thus key. There is very useful work underway between the Commission, EDPS and the Article 29 Working Group with the APEC Data Privacy Subgroup to explore how EU Binding Corporate Rules and APEC Cross Border privacy Rules may interoperate. The process is not an attempt to diminish privacy rules, but rather to find ways to recognize the level of validated compliance in other regimes as part of demonstrating adequate compliance with EU requirements. Such cross-recognition would greatly accommodate companies operating in multiple jurisdictions and facilitate EU growth within the global economy as well as provide benefits to consumers regardless of their country. We urge the drafters to consider how to minimise the administrative burden related to safeguards on international data flows and recognition of regimes. 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.
- Greater guidance on 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.

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 contexts and business models.
- While there is a general recognition of the need to enhance credible enforcement mechanisms, the current proposal lacks proportionality in the specific proposals on sanctions and fines 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 fines (within the range specified for the type of infraction) may not allow mitigating factors and the context of the acts to be properly taken into account. Remedies 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.

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.
- New independent obligations on processors, which would create confusion as to obligations and responsibilities between controllers and processors, should be reconsidered in favour 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.

We welcome the opportunity to provide more detailed comments outlining substantive concerns on these topics as well as other issues of more immediate concern to specific companies. We look forward to continued work with the EU Council, Parliament, Member States, and the Commission in the further enhancement of a Regulation that serves the data protection and economic interests of the EU and its citizens.

The Trans-Atlantic Business Council (TABC) is the largest transatlantic business association, wholly funded by over 70 global companies based in North America and Europe. Our mission is to promote a barrier-free transatlantic market that contributes to economic growth, innovation and security; to foster discussion and the exchange of ideas among business and government leaders; and to serve as a platform for engaging others in the global economy. The TABC is the main business interlocutor to both the U.S. Government and European Commission on international trade and investment issues. We stand out as the only transatlantic business organization uniquely placed to provide one voice for EU and U.S. companies in the Transatlantic Trade and Investment Partnership (T-TIP).