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

AmCham EU's response to the Commission communication on a comprehensive approach on data protection in the European Union

INFORMATION PAPER

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
Register ID: 5265780509-97
Email: info@amchameu.eu

Secretariat Point of Contact: Shannon Petry, shannon.petry@amchameu.eu
Tel: 02 289 10 36

Introduction 3
Executive Summary 5
1 One comprehensive framework 11
1.1 Architecture 11
1.2 Applicable law 11
2 Principles 13
2.1 Technological neutrality 13
2.2 Accountability 14
2.2.1 Accountability is not a new concept 14
2.2.2 Privacy culture 15
2.2.3 Accountability in practice 15
2.2.4 Existing components of accountability 16
(i) Training and policies 16
(ii) Data Protection Officers 16
(iii) Binding Corporate Rules 16
2.2.5 Privacy by Design Process 16
2.3 The importance of context 18
2.3.1 Context provides meaning 18
2.3.2 Context for what? 18
2.3.3 Opt-in vs. Opt-out 20
2.3.4 Legislating for context 20
2.4 Data breach notifications 21
3 Data subjects' rights 22
3.1 Data portability 22
3.2 The right to be forgotten 23
4 Enhancing the Internal Market and Promoting Competitiveness 25
4.1 Better harmonisation: increase legal certainty 25
4.1.1 Definitions 25
(i) Personal data 25
(ii) Consent 27
4.2 Reducing the administrative burden 27
4.2.1 Notifications 27
4.2.2 Privacy notices 28
4.3 Self-regulation 29
4.4 Promoting Competitiveness 31
4.4.1 Promoting dialogue between regulators and industry 31
4.4.2 Accountability for economic development in policy making 32
5 Addressing globalisation and international data flows 32
5.1 Cloud computing 32
5.2 International data flows 35
5.2.1 Adequacy vs. adequate safeguards 35
5.2.2 Binding Corporate Rules 36
5.2.3 Binding Safe Processor Rules 38
5.2.4 Safe Harbor 38
5.2.5 Standard Contractual Clauses 39
5.3 Universal principles 40
6 Cooperation and enforcement 40
6.1 Better cooperation between DPAs and EU authorities 40
6.2 Harm-based enforcement 41
6.3 Class actions 41
7 Conclusion 42

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

INFORMATION PAPER

14 January 2011

Introduction

This document contains the response of the American Chamber of Commerce to the European Union (AmCham EU) to the Consultation on the European Commission's comprehensive approach on personal data protection in the European Union. It follows the Position Statement and Information Paper submitted for consideration during the previous round of consultations on data protection.[1]

AmCham EU recognises that the two main purposes of Directive 95/46 (to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data, and to ensure the free flow of personal data between Member States) remain sound and should always be kept in mind in the preparation of the comprehensive approach on personal data protection currently being suggested.

While the Commission's Communication adequately portrays the challenges posed by innovation and advancing technological changes to application of the Directive, it seems to overplay the utility of increased transparency and enforcement alone to address these challenges. The Communication highlights the need for harmonisation among a myriad of national interpretations of the Directive, including the minimisation of national gold-plating of data protection requirements, increased emphasis on flexible cross-border compliance solutions and consideration of broader global trade implications from EU rules, but does not develop significant discussion to address these 'growing pains' under the Directive commensurate to their importance.

Our comments below – particularly in the areas of better harmonisation, accountability, data portability, notifications and international data flows – focus on the environment in which the Directive operates today, one of increasingly globalised commerce and transactions of personal information. Addressing the 'growing pains' highlighted above will be key to the meaningful transparency and effective enforcement that the Commission seeks in this new environment, not only for the betterment

[1] See '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.

of data subjects and the protection of their data, but also in terms of the proportionality of compliance burdens for controllers and processors.

In a world where information has become a valuable resource in society and where information sharing that serves legitimate purposes is general practice, AmCham EU would like to note that ensuring appropriate protection for collected and processed information is a priority. AmCham EU member companies take data protection seriously and it is an essential element of maintaining user trust and confidence. AmCham EU finds that too often discussions of data protection begin with the false assumption that, in general, personal data is not appropriately protected.

The data minimisation principle, which is based on the assertion that there is no need to protect what has not been collected, can be a useful part of a Privacy by Design approach to protecting personal data. However, it should not be elevated to an obligation, because it might in practice prevent consumers from reaping the benefits that secure collection of personal data can yield. Furthermore, determining the appropriate 'minimum' would be highly subjective and therefore impossible to effectively regulate. Therefore, more emphasis should be placed on determining whether the purposes for data collection are legitimate and specified in ways that are meaningful and understood by data subjects.

AmCham EU believes that the EU should be more ambitious when seeking to reconcile effective protection of privacy and personal data with its economic needs. In a knowledge-based society where 'every European is digital', it is critically important that data protection rules are interpreted and implemented in a way that is respectful of European citizens' legitimate expectation that the EU will protect their prosperity as well as their privacy. This is not just about ensuring the coherence of the Single Market; it is essential to ensuring that the Single Market remains competitive.

A right balance between the protection of personal information and the free flow of information as inspired by Directive 95/46 should remain a key driver of the comprehensive approach on personal data protection in the European Union to the benefit of EU citizens.

Executive Summary

	Issue	AmCham EU's Position
One Comprehensive Framework	*Architecture*	AmCham EU is strongly opposed to a regime where various data protection rules apply per sector and/or per Member State and would not support the introduction of any specific rules that do not fit with the notion of a comprehensive framework.
	Applicable Law	A comprehensive approach on data protection should enable companies operating within various EEA Member States to be subject to one set of data protection rules and therefore concentrate their compliance efforts in a consistent and effective way with one regulator. This would allow businesses operating across borders to save enormous resources without infringing on data subjects' right to privacy.
Principles	*Technological Neutrality*	Retaining the technological neutrality principle throughout the legal framework will enable both Member States and industry to address issues as and when appropriate. Consumers also benefit from technology neutrality, as they will be able to understand the privacy framework and protections regardless of the specific type of device or technology being used, increasing consumer confidence and promoting economic growth. This will ensure that the EU's legal framework for data protection can remain appropriate and effective in the long term.
	Accountability	AmCham EU supports including

		the principle of accountability in new legislation provided accountability is interpreted as a concept underscoring the renewed focus of the legislative proposals on a results-based system. The legislation should also provide the right incentives to organisations to implement the necessary procedures while rewarding those that have taken these steps already.
	Privacy by Design Process	AmCham EU believes that a Privacy by Design Process concept should focus on making sure that organisations (public and private) have implemented privacy protection into training programmes for people and have embedded it in processes. It should not take the form of design mandates or technology preferences, nor focus on prescriptive details regarding services and/or products.
	Context	AmCham EU believes that EU legislators should enable data controllers to take context into account when selecting the most appropriate way of providing information, obtaining consent and offering control.
	Data Breach Notifications	AmCham EU believes that the wider introduction of any data breach notifications needs to be carefully assessed; if the requirements are too broad, breach notifications could be very burdensome to businesses and confusing for/ignored by citizens. AmCham EU recommends that a specific threshold, such as a requirement of a significant risk of harm to the user, be set to

		ensure that notices are effective. AmCham EU also favours a standardised EU data breach notification over a range of different notification obligations across the Member States.
Data Subjects' Rights	*Data Portability*	AmCham EU is concerned about the implementation of an explicit right to data portability in practice and would like to ensure that such a possibility is granted only to the extent it is reasonably technically feasible and that no specific interoperability standards would be imposed on data controllers.
	The Right to Be Forgotten	AmCham EU believes that there needs to be a more open and in-depth debate between stakeholders and policy-makers on a possible legal definition of a 'right to be forgotten' before its introduction into EU law is considered.
Enhancing the Internal Market and Promoting Competitiveness	*Better Harmonisation*	The new framework should address harmonisation issues to enable businesses to take a Europe-wide view of data protection compliance.
	Reducing the Administrative Burden	AmCham EU applauds the intended simplification of the notification regime and the harmonisation of content of information notices. In particular, with respect to notifications, AmCham EU believes that the European Commission should evaluate the need and rationale for *ex ante* notifications and weigh that against the significant and time-consuming burden this creates for controllers and Data Protection Authorities who need to review the large quantities of

		notifications that are filed. For 'riskier' or more sensitive data processing where notifications may be warranted, AmCham EU urges the European Commission to work with Data Protection Authorities to develop harmonised and simplified filing templates at the EU level. Any templates developed should be given mutual recognition across all Member States in order to reduce administrative burdens if or when notification is required. While guidelines regarding privacy notices for users/consumers would be welcomed, AmCham EU would like to caution against standardised compulsory privacy notices drafted without stakeholders' involvement or outside their control.
	Self-regulation	AmCham EU recommends that the Commission take a much more active role in promoting self-regulatory and co-regulatory mechanisms.
	Promoting Competitiveness	In order to promote the EU's competitiveness, the Commission should be given explicit responsibility for ensuring compatibility of the implementation and interpretation of EU data protection law with EU economic and other policy objectives.
International Data Flows	*Accountability-based Regime*	AmCham EU would welcome the opportunity to explore the concept of an accountability-based transfer regime, providing sufficient safeguards and replacing adequacy for international data flows, in more

		detail with the Commission.
	Binding Corporate Rules	AmCham EU believes that, in general, the BCR process can be a useful tool, but calls upon the EU to promote a less burdensome process and a broadening of their scope of application (e.g. not limited to intra-group transfers and coverage of transfers to processors) in order to realise the full potential of this data transfer solution and accountability tool.
	Binding Safe Processor Rules	AmCham EU calls for a flexible internal governance model for data transfers to processors. AmCham EU sees BSPRs as a potentially useful tool in this respect and is ready to contribute to and discuss the outcome of the current work undertaken by European authorities. However, care must be taken to avoid a BSPR procedure that would maintain the complexities and costs associated with today's BCR approval process.
	Safe Harbor	AmCham EU would like to see the Safe Harbor programme recognised as a successful tool in this revision.
	Standard Contractual Clauses	The utility of SCCs could be further improved by giving the parties more flexibility to make changes to SCCs as long as the parties to the SCCs remain the same and there are no amendments to clauses made mandatory by the European Commission.
Cooperation and Enforcement	*Cooperation*	AmCham EU welcomes the work currently being undertaken by the Article 29 Working Party in relation to cooperation between DPAs. It is crucial that DPAs

		better coordinate their activities and cooperate more closely, especially with respect to cross-border matters.
	Harm-based Enforcement	AmCham EU believes that formal considerations of harm to data subjects should be a prerequisite for modern legislation as well as for any enforcement action, most notably for imposing fine.
	Class Actions	AmCham EU cannot support any language that leaves open the possibility of class action suits.

1 One comprehensive framework

1.1 Architecture

AmCham EU recognises the need for a comprehensive and coherent approach to data protection in the EU and welcomes the new consultation issued by the European Commission in this respect.

Given the lack of harmonisation between Member States in this matter after 15 years of implementation of Directive 95/46, AmCham EU is open to the Commission examining the possibility of proposing a Regulation, rather than a new Directive, to develop the new comprehensive framework in a single instrument. This would avoid the risks created by varying implementation among Member States as the same rules would then be directly applicable in all Member States. However, AmCham EU is mindful of the fact that the content of the legislation will be a relevant factor when determining the most appropriate legal instrument. We believe that the most appropriate choice will become clearer as the text materialises.

AmCham EU suggests that EU authorities examine the possibility of an opt-for regime, available to companies that operate across the EU. This regime would enable companies to have a single set of rules applicable across all their EU activities, as is the case of the alternative method for harmonising national laws (known as the 28th regime) which has recently been referred to in the context of the revision of the draft Consumer Rights Directive.

AmCham EU is strongly opposed to a regime where various data protection rules apply per sector and/or per Member State and would not support the introduction of any specific rules that do not fit with the notion of a comprehensive framework.

1.2 Applicable law

The applicable law rule set forth in Article 4 of Directive 95/46 has proved difficult to apply in practice, particularly when several Member States are concerned or when 'equipment' is used in the EEA by a data controller that is not established in the EEA.

Under the current framework, when data collection by one company takes place in various EEA Member States with the

involvement of its European affiliates or equipment in the EEA, that company may have to comply with the rules applicable in each country where data collection takes place. This creates uncertainty as well as adding to the compliance burden.

AmCham EU calls for a review of the applicable law principle whereby the applicable rules should only be those of the EEA country where the company's 'main establishment' is located.[2]

Such a principle would mean that a multinational company is subject only to the law and enforcement agency of its 'main establishment's' home state. Only that Member State's law would be applicable to the EEA operations and to any EEA subsidiary (assuming majority ownership and control of that entity) and only the multinational's EEA home state data protection authority should have the ability to take action against that company (regardless of the location of any individual subsidiary location, if any). Such a principle would be of huge benefit to the data protection regime overall, bringing greater legal certainty to companies and end users.

AmCham EU believes that a clear definition of the concept of 'main establishment' of a company must be provided in the new framework. AmCham EU is ready to work with the Commission to identify the considerations that may be relevant to define a 'main establishment' (e.g. main operations in the EEA, main location for business purposes in the EEA, where the physical operations are based, where personal data is processed and/or where decisions about data processing are made).

To create greater legal certainty for both users and companies, it is essential that the overall regime be harmonised. Greater consistency across the EEA would give national data protection authorities the confidence that the application of another Member State's law adequately protects the personal data of their own citizens.

A comprehensive approach on data protection should enable companies operating within various EEA Member States to be subject to one set of data protection rules and therefore concentrate their compliance efforts in a consistent and effective way with one regulator. This would allow businesses operating

[2] The Article 29 Working Party also supports such a principle, as indicated in its Opinion 8/2010 on applicable law adopted on 16 December 2010.

across borders to save enormous resources without infringing on data subjects' right to privacy.

2 Principles

In addition to the key principles already set forth in Directive 95/46, AmCham EU believes that the following principles should be included in the comprehensive legal framework: technological neutrality, accountability, the importance of context and data breach notifications.

2.1 Technological neutrality

In its Communication, the Commission recognises that any changes to be made to the legislative framework in this current review will have to "stand the test of time", just as Directive 95/46 has. AmCham EU agrees with the Commission that the legal framework must provide legal certainty to citizens of future generations regardless of how sophisticated technology may become. To ensure this is possible, it is important that the technology-neutral approach that has been shown to be effective is maintained and is neither removed nor unintentionally called into question.

While AmCham EU finds it appropriate for the current review to consider the challenges of today's technology, such as social networks and cloud computing, we suggest that the review also look beyond current technologies in order to ensure that the legal framework will be appropriate regardless of specific technologies that might come of age in the future. This requires the retention of the technological neutrality principle as well as the avoidance of any introduction of requirements focused on a specific technology or possible technology mandates.

For example, while Privacy by Design is a concept that AmCham EU supports in principle, it is important that this concept not be defined in the legal framework in a way that demands technology-specific requirements for the design and deployment of IT products or solutions. A definition that goes into details and specifics as to the technology that should be embedded or bundled into IT equipment could tie the hands of industry, preventing it from developing innovative privacy tools and solutions to address threats and risks to data protection, security and privacy that may not even be envisaged today.

It should be remembered that information is a key target for criminals, whose activities evolve and adapt much more quickly than legislation can be changed. Prescriptive requirements could impede industry efforts to counteract criminal activity and, in the end, would be counterproductive.

Retaining the technological neutrality principle throughout the legal framework will enable both Member States and industry to address issues as and when appropriate. Consumers also benefit from technology neutrality, as they will be able to understand the privacy framework and protections regardless of the specific type of device or technology being used, increasing consumer confidence and promoting economic growth. This will ensure that the EU's legal framework for data protection can remain appropriate and effective in the long term.

2.2 Accountability

2.2.1 Accountability is not a new concept

Accountability refers to the ability of company to demonstrate its capacity to achieve specified privacy practices and to have that capacity objectively measured by regulators or internal/external auditors. The concept of accountability already exists and is used today; a limited example is Binding Corporate Rules (BCRs), where companies (data controllers) show regulators how their internal rules protect personal data and be measured on how these rules are upheld.

Accountability also applies with respect to security measures to be implemented by data controllers and processors and to the appointment of data protection officers pursuant to the current data protection directive.[3]

[3] One example can be found in Canadian legislation: 'Canada has, through the Personal Information Protection and Electronic Documents Act (PIPEDA), chosen an organization-to-organization approach that is not based on the concept of adequacy. PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. However under PIPEDA, organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement. The Office of the Privacy Commissioner of Canada can investigate complaints and audit the personal information handling practices of organizations'. *See* www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.cfm.

The European Commission should examine how these tools can be used in a more harmonised and predictable fashion.[4]

2.2.2 Privacy culture

AmCham EU calls for the regulatory framework to move from a procedure-based regime to a results-based legal system. In such a system, legislation should establish general guidelines for the outcome to be achieved; it should not focus on the precise means for achieving this via administrative and overly prescriptive processes that do not necessarily lead to increased data protection.

In a results-based system, public and private organisations are accountable for handling data wherever that data travels. This will allow them to focus on the core objective of the legal framework instead of merely seeking legal compliance.

Additionally, accountability and liability should be recognised as distinct principles. Accountability should not result *a priori* in liability; additional legal steps should be necessary to establish liability on a case-by-case basis beyond demonstrations of accountability mechanisms.

An improved legal framework should encourage and give incentives for organisations to be held accountable. Such organisations should set the protection of individuals' rights as a recognised corporate objective, while seeking and achieving legal compliance. This will enable data protection to become a proactive part of all businesses rather than a reactive compliance function. Ensuring that this accountability follows the data, regardless of where it is controlled or processed, will ultimately increase data protection and benefit all consumers.

2.2.3 Accountability in practice

AmCham EU favours the introduction of accountability principles. The concept of accountability that AmCham EU calls for is, however, broader than that mentioned in the Communication, which is only focused on increasing the responsibility of data controllers. Rather, we believe accountability is a concept that should be the foundation of the

[4]At the international level, the accountability principle has already been recognised in the OECD Privacy Guidelines first established in 1980 and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

legal framework in its totality, of how we look at data protection, of how we enforce it and of how we supervise it.

We also stress the need to allow companies the flexibility to determine how accountability should be demonstrated depending on the business model, sector or systems already in place.

AmCham EU supports including the principle of accountability in new legislation provided accountability is interpreted as a concept underscoring the renewed focus of the legislative proposals on a results-based system. The legislation should also provide the right incentives to organisations to implement the necessary measures while rewarding those that have taken these steps already.

2.2.4 Existing components of accountability

(i) Training and policies

AmCham EU believes that staff training and policies could be part of an accountability model.

(ii) Data Protection Officers

AmCham EU recognises that the appointment of an internal Data Protection Officer within a group of companies can conform with the accountability model. However, a strict obligation to appoint a Data Protection Officer may not be implementable; there is immense variation across companies' internal structures and business models. In some cases, companies may be able to find ways to protect personal data that are more effective than the appointment of a Data Protection Officer.

(iii) Binding Corporate Rules

Possibly the best (albeit of limited application) example to date of an accountability-based mechanism founded on an internal governance approach across the organisation in the framework of Directive 95/46 is the Binding Corporate Rules data transfer solution which some AmCham EU members currently have in place.

2.2.5 Privacy by Design Process

AmCham EU underlines the importance of implementing and integrating accountability in the development of organisational systems and processes. Privacy by Design Process (PbDP) is a concept that should be part of an accountable company's overall approach to supporting privacy in an environment of

technological change and information-intensive innovation. AmCham EU is supportive of a drive for organisations to embed PbDP into their processes and people.

To date there is only a vague definition of PbDP available in the EEA and all stakeholders would need to be involved in fully defining the concept. Indeed while PbDP has become a popular term in the privacy community, it means different things to different people.

There is a clear need to look at the issue of data protection with a global perspective to avoid further fragmentation, taking stock of industry's own efforts and taking into account technological developments. Although every organisation should integrate privacy into its processes, the rules should allow for flexibility and leave room for adaptation in how this is done. This is especially the case with respect to small and medium-sized enterprises (SMEs) given their specific business processes and resources. One should keep in mind that there is not one single way of implementing Privacy by Design Process and that the different elements of a company's process should be taken into account. PbDP does not just describe how the products are built; it reflects how services operate and how business is conducted.

In that context, AmCham EU supports the concept of Privacy by Design but thinks any reflection on the concept in legislative proposals should provide the flexibility necessary to account for different business models and organisational needs. It should focus on designing privacy into processes and people and should not impose 'privacy by default' or any technology mandate. AmCham EU would like to work with all stakeholders to further define the concept and provide the European Commission with input regarding its implications.

We would further like to stress that all legitimate businesses already have processes in place that would fall under the concept of Privacy by Design Process (ranging from more formal and documented procedures such as Privacy Impact Assessments to internal controls, regular interactions between the legal department and the technology developers or simply the existence of privacy officers). These should be acknowledged, allowed and encouraged if any PbDP concept is introduced with the legislative revision. The most appropriate specific mechanisms to ensure effective PbDP measures within a business (and ultimately a high level of data protection for data subjects) will always be best

determined by the business itself depending on factors such as the type of personal data processed as well as the business model, sector and size of the company.

AmCham EU believes that a Privacy by Design Process concept should focus on making sure that organisations (public and private) have implemented privacy protection into training programmes for people and have embedded it in processes. It should not take the form of design mandates or technology preferences, nor focus on prescriptive details regarding services and/or products.

2.3 The importance of context

Since 1995, a significant transformation of society and the global economy has led to an explosion of the number of contexts in which data, including personal data, is collected and processed. This proliferation of contexts is one of the main drivers for change in the legislative framework. It is therefore important that legislators take the issue of context into account when drafting new texts.

2.3.1 Context provides meaning

Effective communication is at the heart of economic and social progress, and effective communication is impossible without a mutually understood context. This is a reality that we experience in everyday life. Context is what makes a joke funny for those who share it. The importance of context is also something keenly understood by anyone who has been quoted out of context in the media. Interactions between data subjects and data controllers are not an exception to this – effective protection of privacy is therefore also heavily dependent on context.

2.3.2 Context for what?

Data subjects must understand the context in which they are *provided information* by data controllers about the collection and use of data. This might be as simple as seeing the logo or brand of a data controller on a letterhead (for example, most people will immediately understand the context of a bill from a utility company before even opening the envelope). It could also be a more complex situation, such as the collection of data by a familiar data controller (e.g. employers, websites, retailers) for a previously unspecified purpose. In some cases, context for

data collection and use is particularly hard to explain. This can be the case, for example, when an unfamiliar party seeks to collect data. In such cases, providing notice and transparency in context is arguably even more important, since the data subject is otherwise unlikely to understand. Seen from another angle, transparency and information-sharing are worth nothing if provided out of context. An employee cannot be expected to understand information provided by his or her employer if it is provided in the street on a holiday.

According to Directive 95/46, *consent* must be freely given, specific and *informed* in order to be valid. This last characteristic is the one that is most dependent on context. As described above, information provided out of context is unlikely to be a basis for valid consent. The concept of *implicit consent* is also heavily dependent on context. It should also be noted that the validity of consent may or may not have a temporal dimension (e.g. in some contexts, consent for use of data collected can conceivably be valid if it is given before, during or after data collection, especially if the data is collected for other purposes). In a fast-moving world of innumerable data-enabled transactions, context has become an essential element for providing valid consent.

The Article 29 Working Party (A29WP) has already acknowledged the importance of context in relation to consent in its work on consent provided in the context of an employment relationship.[5] Consent in a particular context is often linked to the desire to ensure a certain 'benefit' within that context; and this should not be understood as 'trading' privacy. A good example is healthcare: if a patient can receive better, more accurate and more effective treatment with the use and processing of their personal data combined with hospital data and research data, they may want to consent to that data being used as long as security safeguards are in place. Today, interpretation of this part of Directive 95/46 varies across the Member States, and improved consistency is needed.

The logic of context also applies to data subjects' *control* over their data. Like any other type of communication, an opportunity for data subjects to affirm or refuse the

[5] Opinion 8/2001 on the processing of personal data in the employment context, DG MARKT 5062/01, 13 September 2001.

collection and use of data needs to be done at a time and in a place that makes sense and is in line with the data subject's reasonable expectations.

2.3.3 Opt-in vs. Opt-out

It is an unfortunate fact that the old framework, with its insufficient emphasis on context, has created a polarised debate between those in favour of 'opt-in' approaches to consent and control (broadly defined as ruling something out unless the data subject has expressly chosen to accept it) and those in favour of 'opt-out' (broadly defined as a situation where the data subject is allowed to stop something that would otherwise proceed). 'Opt-in' has come to be perceived as more protective of users' privacy than 'opt-out'. The result has been a drive by privacy advocates (and indeed by many legislators) to push for 'opt-in' approaches to data protection to become the norm. In recent years, however, it has become clear that a poorly designed 'opt-in' (for example, one provided out of context) is less protective of privacy than a well-designed 'opt-out'. Indeed, there is currently a wide range of mechanisms that enable users to control and consent to use of their information; some of the more robust opt-out mechanisms in fact do a better job of protecting privacy than do weaker opt-in mechanisms.

A good example of this would be the transparency and control tools that are being developed by the online advertising industry specifically for behaviourally targeted ads. Both transparency and control will be provided contextually where the user would intuitively expect and understand them – in the ads themselves. By clicking on a globally standardised icon located in or around the ad, users will be able to access detailed information about behavioural advertising and exercise control over it via an industry-wide tool that will stop the delivery of such ads to that user's browser. This kind of context-sensitive approach potentially frees us from the sterile 'opt-in vs. opt-out' debate by both better protecting the data subject and allowing for new business models to develop responsibly.

AmCham EU believes that EU legislators should enable data controllers to take context into account when selecting the most appropriate way of providing information, obtaining consent and offering control.

2.3.4 Legislating for context

The challenge of context for legislators is that it is so infinitely varied, intangible and changing that it is actually impossible to lay down detailed rules for a case-by-case analysis of its impact. Thankfully, the legislative framework is principles-based and provides the flexibility needed to apply rules with common sense to the relevant situation. The principles-based approach must continue in order to provide the necessary flexibility. However, this flexibility must not be seen as a license for data controllers to act irresponsibly. Effective self-regulation is needed in many areas where context has a particular impact, such as in the example of behavioural advertising addressing in section 2.3.3.

AmCham EU urges the European Commission to explicitly recognise the role and importance of context as a critical factor for data controllers to take into account.

2.4 Data breach notifications

AmCham EU sees the introduction of a data breach notification provision across all sectors as a tool for increasing transparency and consumer understanding. Introducing a requirement in the legal framework to notify users if data has been lost or stolen can empower consumers to take action if they want or need to.

It is important, though, to consider the threshold above which the need to notify would apply when drafting an appropriate and workable notification framework. Determining the level at which a breach would be serious enough to trigger a notification provides clarity to organisations in terms of what action is expected of them and when. It can also help address concerns with respect to possible over-notification of citizens. AmCham EU suggests that, moving forward, the Commission considers introducing the principle of a 'significant risk of harm' threshold.

However, AmCham EU would like to caution that the details and specific procedures to be followed should a horizontal data breach notification requirement be introduced need to be discussed in detail with stakeholders. If notice obligations apply to data or events that do not constitute a significant risk of harm, over-provision of notices could confuse consumers and, with time, potentially lead them to ignore important notices. Notifications can be a burdensome, complex and costly procedure for businesses, data protection authorities (DPAs) and citizens so the modalities need to be well thought-through (especially if such an obligation were to apply across the public and private sectors).

The legislative framework should also explicitly recognise the important role that privacy and security technologies can play in protecting data that is lost or stolen. For example, if the data lost is encrypted, the notification requirements associated with that breach could be adjusted accordingly to account for the reduced risk of harm.

The right balance must be found between breach notification as a means to improve appropriate security measures or sanctions and any remedial actions implemented in order to minimise harm, disruption and reputational consequences. In this context, entity or group internal disclosures should not be considered unauthorised disclosures (unless they relate to a specific individual and therefore could be subject to a data subject request).

AmCham EU believes that the wider introduction of any data breach notifications needs to be carefully assessed; if the requirements are too broad, breach notifications could be very burdensome to businesses and confusing for/ignored by citizens. AmCham EU recommends that a specific threshold, such as a requirement of significant risk of harm to the user, be set to ensure that notices are effective. AmCham EU also favours a standardised EU data breach notification over a range of different notification obligations across the Member States.

3 Data subjects' rights

In addition to the rights already granted to data subjects by Directive 95/46, which are already effectively implemented in practice by AmCham EU members, two 'new' data subjects' rights are mentioned in the Communication: data portability and the right to be forgotten.

3.1 Data portability

AmCham EU understands the interest data subjects have in the possibility of withdrawing their data from one application or service in order to transfer this withdrawn data into another application or service. Some companies already voluntarily provide this as a service.

AmCham EU is concerned about the implementation of an explicit right to data portability in practice and would like to ensure that such a possibility is granted only to the extent it is

reasonably technically feasible and that no specific interoperability standards would be imposed on data controllers.

3.2 The right to be forgotten

The Communication calls for clarification of the 'right to be forgotten', i.e. the right of individuals to have their data no longer processed and deleted when it is no longer needed for legitimate purposes.

AmCham EU notes that the elements of the so-called 'right to be forgotten' are already enshrined in the current Directive, in so far as this concept is considered from a privacy and data protection perspective. Indeed, the obligation to keep data only as long as necessary for the purposes for which the data has been collected, along with the right to have data deleted and the right to withdraw consent, are components of the 'right to be forgotten'.

These provisions may not yet have lived up to expectations due to implementation and enforcement failures, but AmCham EU does not believe that this justifies the introduction of a 'right to be forgotten', which inherently carries much wider ethical and philosophical connotations.

AmCham EU agrees that there may be a need to reinforce the existing rules, but argues that the 'right to be forgotten' seems to have introduced a debate that deviates from the heart of the problem. AmCham EU would like to caution against an attempt to address all the societal challenges of the 'right to be forgotten' exclusively through creation of unjustified obligations on data controllers and processors. For instance, some lines of thought currently being developed at the Member State level would inevitably lead to a general obligation to monitor the Internet, undermining the strong foundations on which the Internet was developed in the first place and the basis on which democratic societies operate. Such a debate may be valid as technology has penetrated every aspect of our lives, but certainly should not be held in the context of the revision of the EU legal framework on data protection. In fact, it has already been addressed in the Commission's recent consultation on e-commerce. It should be noted that the e-Commerce Directive prevents the imposition of a general obligation to monitor on website providers, and that this provision was an integral part of the excellent balance of rights and responsibilities that was struck at the time.

AmCham EU believes that it would be useful for the European Commission to focus on substance rather than joining a rhetorical debate. A clarification of the 'right to be forgotten' as meaning that individuals have the right 'to have the data they provide no longer processed and deleted when it is no longer needed for legitimate purposes' would be welcome.

To be workable, the rights to data portability and deletion must clearly distinguish between data directly inputted by the user (e.g. photos or names of friends) and data created by the service provider. The scope of "user data" will need to be clearly delineated in close consultation with industry in order to avoid differences of interpretation and approach across the Member States.

AmCham EU believes that there needs to be a more open and in-depth debate between stakeholders and policy-makers on a possible legal definition of a 'right to be forgotten' before its introduction into EU law is considered.

At this stage, we see that such a right may lead to serious practical difficulties and undesirable or unintended consequences. Many questions remain unanswered, including:

- What types of data should fall under such a right? Introduction of the right may be triggered by current privacy concerns (particularly related to social networks) but how would it apply to the rest of the online (and even offline) world?
- What would happen with metadata or back-up systems if a 'right to be forgotten' is introduced in EU law?
- What level of anonymisation would be acceptable for the right to be inapplicable?
- How would the 'right to be forgotten' be enforced in the public sector?
- How would it be reconciled with other legal requirements relevant to law enforcement, such as data retention requirements?
- How can both the public and private sectors handle the legal, financial and technical complexities that such a right would entail?

One suggestion recently raised to address technical complexity, expiration dates for information, at this stage seems entirely unworkable and does not at all take into account the societal and economic benefits that derive from the analysis and secondary uses

of the vast amounts of data produced in our daily activities (not to mention the technical challenges it entails).

Finally, AmCham EU strongly supports Commissioner Kroes' views on this topic, as expressed in her speech of 25 November 2010 on cloud computing and data protection: 'Just like in real life, when you present yourself on the net, you cannot assume no records exist of your past actions'.

4 Enhancing the Internal Market and Promoting Competitiveness

4.1 Better harmonisation: increase legal certainty

Personal data processing is currently regulated in fragmented ways across the EEA due to differing implementations and/or interpretations. Each Data Protection Authority has their own interpretation of the broad principles of the Directive, based on their local legal and cultural expectations. There has been a growing lack of legal certainty regarding how Member States are interpreting fundamental core principles of the Directive, such as the definitions of personal data and consent.

The new framework should address harmonisation issues to enable businesses to take a Europe-wide view of data protection compliance.

4.1.1 Definitions

Some existing definitions in Directive 95/46 may need to be revised to ensure a better harmonisation and increase legal certainty.

(i) Personal data

The concept of personal data is at the forefront of the discussion of the review of the data protection Directive. Indeed, the presence and processing of data that is considered personal in accordance with the definition spelled out in the Directive triggers the application of the set of rights and obligations outlined in the Directive. The broad and imprecise character of the current definition creates a level of uncertainty regarding the extent to which those rights and obligations apply to particular cases. This

lack of clarity is highlighted in the Communication as well.

A more nuanced approach to the concept of personal data is needed, going beyond the binary system currently in place. The key is to determine a system that addresses what rights and obligations are necessary (appropriate and proportionate) to protect the information processed. AmCham EU suggests a few concrete alternatives that may deserve consideration when drafting the proposal to review the Directive:

- Creation of objective criteria that, if met, would determine not only if data is personal but also the context in which data becomes personal. This concept is already enshrined in Austrian law.[6]
- Maintenance of the current definition, complemented by the creation of a gradation system of obligations based on the risks of harm to individuals through the processing of information related to them.

Additionally, AmCham EU asks the Commission to explicitly exclude business contact information (names, office addresses, email addresses and telephone information – and, as the case may be, company names) from the definition of personal data. Contact information should not be qualified as personal data. Enterprises need to use business contact information to conduct business; it is indispensible to reach their customers, to coordinate with their suppliers and to work with business partners. Currently, enterprises must obtain consent for the processing of such data. The Spanish Data Protection Authority has recognised that this is an excessively cumbersome requirement and has excluded business contact information from the scope of personal data in Spain. AmCham EU encourages the Commission to ensure that this exclusion is applied across the EU. This simple step

[6] See the definition of 'only indirectly personal data' used to refer to data which relate to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means, available at http://www.ics.uci.edu/~kobsa/privacy/Austrian-english.htm#E1

would immediately reduce the burden of compliance at little real cost to personal privacy, as the data relates only to contact information of individuals at their places of business.

(ii) Consent

Directive 95/46 describes consent as 'freely given, specific, and informed'. AmCham EU believes that this definition remains entirely appropriate, and allows for the flexibility that is necessary in the modern world.

However, the existing framework insufficiently emphasises the importance of context (see section 2.3 above). Traditional interpretations of consent have tended to give primary importance to the temporal aspect of consent at the expense of other crucially important contextual factors. This emphasis is based on an assumption that has fed the polarisation of the "opt-in vs. opt-out" debate, but which has not actually protected or empowered data subjects.

AmCham EU calls on the Commission to clarify that the validity of consent depends heavily on context. EU legislators should seek a modern approach to consent that allows data controllers to select the most contextually appropriate way of providing information, obtaining consent and offering control. This could allow the debate to move on from "opt-in vs. opt-out" while better protecting the data subject and allowing new business models to develop responsibly.

4.2 Reducing the administrative burden

AmCham EU applauds the intended simplification of the notification regime and the harmonisation of content of information notices.

4.2.1 Notifications

It is widely recognised that the current notification system needs to be revised and simplified. The significant differences that exist across the 27 Member States, such as the amount of detail required and the type of forms to be used, lead to significant compliance costs and result in

unequal enforcement. As a result, any organisation operating across the EU Member States needs to file separate registrations and consequently cannot benefit from economies of scale.

AmCham EU believes that the European Commission should evaluate the need and rationale for *ex ante* notifications and weigh that against the significant and time-consuming burden this creates for controllers and data protection authorities who need to review the large quantities of notifications that are filed.

Instead, both controllers and data protection authorities would benefit from *ex post* controls which would lead to a system based on compliance and accountability for the protection of personal data.

For 'riskier' or more sensitive data processing where notifications may be warranted, AmCham EU urges the European Commission to work with Data Protection Authorities to develop harmonised and simplified filing templates at the EU level. Any templates developed should be given mutual recognition across all Member States in order to reduce administrative burdens if or when notification is required.

4.2.2 Privacy notices

Transparency is essential to allowing users to make informed and meaningful choices about the processing of personal information related to them. The existing EU data protection Directive lays down the main elements to be contained in privacy notices. However, because of the leeway afforded to Member States in implementing the Directive, there are often additional and differing national requirements to be considered. This means that companies must sometimes have different privacy notices in different Member States, creating an additional administrative burden. It may also prove difficult to ensure complete compliance with the differing rules from a technical point of view.

Nevertheless, AmCham EU would like to caution against any static, detailed provisions in the forthcoming legislative proposal that would impair the creativity and communication of companies' privacy practices. Indeed, AmCham EU believes that the transparency principle should remain as flexible as possible, allowing companies

to *realise* it in their product and service policies in ways that are meaningful to their particular audiences (e.g. consumers and users of a particular product or service). There should be no rigid standardisation of what information is disclosed and how, and security aspects should not be put at risk; if standard privacy notices are drawn up, their use should be left voluntary.

While guidelines regarding privacy notices for users/consumers would be welcomed, AmCham EU would like to caution against standardised compulsory privacy notices drafted without stakeholders' involvement or outside their control.

4.3 Self-regulation

In recent years, the European Commission has increasingly resorted to softer legal instruments such as recommendations as an alternative or ancillary to traditional authoritative legislation. This approach has led to more effective, pragmatic and business-minded actions. Similarly, the European Commission has supported industry initiatives for self-regulation, especially in fast-developing areas of industry.[7]

In order to ensure effective data protection in a rapidly evolving environment, self-regulation is a very effective tool to help data controllers comply with legal rules in practice. It also helps regulators gain a better understanding of how rules should apply in a concrete situation.

Article 27 of the Directive already contains provisions encouraging the adoption of codes of conduct for the proper implementation of legal rules in specific sectors. However, to date, very few industry codes have been developed pursuant to Article 27 of the Directive, even though such mechanisms could play an important role in ensuring strong privacy protection in an era when data routinely moves across jurisdictional boundaries, complicating regulatory efforts by national authorities.

The current system– with detailed national implementation of the Directive in each Member State – has not left much room for the promotion of effective self-regulation. This is presumably because

[7] See for example, the Safer Social Networking Principles for EU and the European Framework for Safer Mobile use by Young Teenagers and Children (http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm).

conscientious Member States prefer to prescribe all means to comply with legal rules rather than leave them to self-regulation by the industry in general or data controllers in particular.

An efficient way to foster effective self-regulation would be to re-visit Article 27 in a way that would encourage Member States to support self-regulation as a valid means of compliance with EU law. Revisions could also consider promoting pan-European self-regulation in order to strengthen the Single Market.

In practical terms, the changes to the current provisions of Article 27 would be as follows:

First, the first paragraph of Article 27 should be supplemented to cover European-level codes of conduct, taking into consideration the recognised need for a more harmonised implementation of data protection rules in each Member State. The process described in the third paragraph of Article 27 as regards Community codes echoes this wider approach and should be reinforced so as to encourage and support pan-European solutions adopted by industry operators.

Second, the roles of the national and EU-wide authorities (such as the A29WP) should be more clearly defined and, given the nature of self-regulation, data controllers, trade associations and other bodies should be able to consult them on a voluntary basis. Self-regulation should indeed remain a voluntary act by operators and should not depend on regulatory approval at the national or European level that could hamper development and effectiveness with complicated and time-consuming procedures. In that respect, according to the current third paragraph of Article 27, approval by the A29WP is based on analysis of compatibility with national laws, a stipulation that seems to actually duplicate the work responsibilities that individual DPAs already have to measure compliance with their national laws.

Third, it should also be made clear that regulators' approval (or not) of codes of conduct is a separate matter from determinations of individual operators' compliance with the law.

Lastly, Article 27 should also be supplemented to incentivise effective self-regulation, for example by acknowledging a limited legal exposure for operators participating in approved self-regulation schemes.

AmCham EU strongly believes that the above changes should be seriously considered. Implementation could be ensured by assigning responsibility for supporting self-regulation from the standpoint of its economic benefits to a section of the Commission or to a new body at the European level.

Besides the above submission procedures of codes of conduct to the regulatory authorities, AmCham EU also favours industry-developed and managed certifications provided they remain voluntary and affordable. Such certifications should be open to companies both inside and outside the EEA in order to facilitate international data flows. Indeed, industry is able to adapt to new market realities at a faster pace than government, and government does not have the same competitive incentive to enforce proper use of certifications (e.g. icons or seals on web pages) as industry does. In the long term, an industry-developed and managed certification that is endorsed by both EU and non-EU regulators would help reduce compliance burdens on operators and foster competitiveness.

AmCham EU recommends that the Commission take a much more active role in promoting self-regulatory and co-regulatory mechanisms.

4.4 Promoting Competitiveness

The current legislative framework created strong institutions whose primary responsibility is to protect privacy. These include the national Data Protection Authorities (DPAs), the European Data Protection Supervisor (EDPS) and his office, and the Article 29 Working Party. These institutions have done stellar work in privacy protection, and are to be commended. However, AmCham EU believes that the EU should always seek to balance complementary policy objectives.

4.4.1 Promoting dialogue between regulators and industry

DPAs and the A29WP are rightly focused on protecting citizens' privacy. Unfortunately, the way these institutions have interpreted the law and the approaches to compliance they have recommended or required have often failed to reflect technological, commercial or economic realities. We believe this is due in part to the A29WP's failure to adequately consult industry during preparation of its opinions and recommendations.

The Commission should therefore propose that Article 30 be amended to include an obligation for the A29WP to consult industry in the preparation of its opinions and recommendations.

4.4.2 Accountability for economic development in policy making

AmCham EU believes that the respective roles and responsibilities of the A29WP and the Commission as described in Article 30 have not been reflected in practice. Accordingly, these provisions on roles and responsibilities should be strengthened and clarified to require the Commission to assess whether the work of the A29WP has potential economic impacts or impacts other EU policy priorities (including industry consultation, effects on competition, the coherence of the Single Market, or the growth of a specific sector or activity). Further, the Commission should respond to the A29WP's opinions or recommendations in cases where it believes they have such an impact. The A29WP should be given the opportunity to revise its opinions or recommendations in light of the Commission's response. If the Commission believes there is sufficient need to clarify or promote a common approach, it should adopt a Commission Recommendation on the subject.

In addition, the Commission should proactively monitor any Member State's transposition and implementation of the legislative framework, with a view to ensuring a consistent and coherent approach across the EU.

The Commission should present an annual report to the European Parliament on Member States' implementation of the legislative framework and its work on ensuring an appropriate balance between the framework's security, economic and privacy objectives.

In order to promote the EU's competitiveness, the Commission should be given explicit responsibility for ensuring compatibility of the implementation and interpretation of EU data protection law with EU economic and other policy objectives.

5 Addressing globalisation and international data flows

5.1 Cloud computing

Cloud computing solutions are currently growing steadily and should grow even more in the coming years, holding great promise for Europe. Cloud computing also offers innovative ways to enhance data privacy and security. However, these technologies also raise a new set of questions about how to best protect user privacy while simultaneously enabling innovation.

AmCham EU agrees with the European Commission that high standards of data protection are needed within cloud computing. Many AmCham EU members are developing cloud services. Without high standards of data protection these services will not be taken up by customers around Europe, meaning the potential of cloud computing will not be fulfilled. However, there are many open questions about cloud computing and its regulation and these cannot all be addressed in the data protection directive review.

Data protection law is based on protecting data in a given physical infrastructure in a fixed location that can be identified and protected. By definition, current data protection rules will struggle to deal with the realities of cloud computing.

Cloud computing is a technology with many definitions, but it is generally understood as referring to computing services provided to customers through the internet. The Commission's Communication uses the definition 'Internet-based computing whereby software, shared resources and information are on remote servers ('in the cloud')'. AmCham EU would agree with this definition but further nuance it by noting that cloud computing can be either Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS). These are, broadly, the main service models of cloud computing. In addition not all clouds are the same. There are public clouds, private clouds and hybrid clouds. Some companies have their own private cloud infrastructure behind their own firewall and governments in Europe are considering this option.

While cloud computing itself is not an entirely new model of computing, its potential is only just being understood. The ability for companies to scale up their computing needs quickly will mean that they can have the processing power they require without having to maintain or purchase infrastructure. Cloud computing, it should be noted, can give access to more expertise as companies can purchase IT security services and have access to

teams of security professionals that the cloud service providers need in order to protect data.

With regard to the Commission's Communication, the main challenge highlighted is the fact that using cloud computing could lead to international transfer of data without the data subject realising that their data has left the country. This touches upon the issue of data transfer outside the EEA that will be discussed in Section 5.2.

Indeed, cloud providers often offer services that transcend geographic boundaries, with data stored on servers in multiple markets, belonging to customers in various jurisdictions and routinely moving across national borders. Differences in national rules on data privacy and security mean that a patchwork of protections, some stronger and some weaker, apply to cloud data. This undermines users' confidence that their data is safe while occasionally creating conflicts between substantive legal obligations imposed on cloud providers.

Several models are available today for the transfer of data outside the EEA. The review of the legal framework is an opportunity to evaluate existing models such as Binding Corporate Rules, the Safe Harbor programme or other international agreements and Standard Contractual Clauses vis-à-vis the cloud and other new challenges, and to propose new ones[8] to ensure that data is transferred with adequate protection.

Another option for managing international data transfers and cloud computing would be to recognise that companies can move data controlled within their own company or corporate group across international borders. Should a company or a cloud service provider undertake to manage data protection for their own data or for a customer's data within their own IT infrastructure, then they should be allowed to move data internationally. The company providing the service would take on responsibility for ensuring data protection wherever the data is stored globally. This also fits with the principle of accountability, where companies have to be accountable for data protection. This model has been recognised in other countries around the world.[9] This would allow cloud computing to develop without obliging governments to redraft complex international data transfer rules.

[8] See discussion of international data flows in section 5.2.

[9] See, *inter alia*, the APEC Privacy Framework, Asia-Pacific Economic Cooperation Secretariat, 2005.

The review of the data protection Directive also affords an opportunity to remove additional requirements for data transfers. A company doing business in the EEA should be subject to one standard in this area, not a range of them as is currently the case. AmCham EU believes that solutions can be found during review of the data protection Directive that will allow the continued development of cloud services with strong data protection requirements.

5.2 International data flows

The possibility of transferring personal data within globally operating companies and the possibility of involving service providers that may be located in- or outside the EEA is a key requirement of the business community. In many cases it will be far more efficient to involve global service providers, which will require personal data to be transferred, stored and processed in third countries.

Companies are sensitive to the need to provide proper protection of the personal data that they process for their customers and employees. Over the last decade, sensitivity both of the public and of company employees as to how their personal data is collected and processed has significantly increased. Companies have both legal and commercial reasons to comply with data protection laws, including a desire to be successful in the marketplace and to be seen as an employer of choice by employees. Although the current text of Article 26 of the Directive allows for a range of derogations, it would be good to take advantage of the opportunity offered by amending the Directive to introduce improvements.

5.2.1 Adequacy vs. adequate safeguards

The Communication highlights a number of inconsistencies which currently exist in the rules regarding international data transfers and which could be addressed by the new comprehensive framework. The recognition of these problems is welcomed. However, AmCham EU regards the proposal to only examine how the adequacy principle could be further clarified and enhanced as a missed opportunity to reconsider whether the adequacy principle is itself adequate and whether it will still have a role to play in the future legal framework.

Information is already being transferred (under contractual arrangements as allowed by the Directive) to non-EU countries that may in fact fail the adequacy test. We believe that the adequacy principle is itself not working. Therefore, the Commission should reassess the need to 'clarify' adequacy procedures and instead examine other means of ensuring data remains protected when transferred internationally.

AmCham EU believes that the adequacy principle could be replaced by the extension of the principle of accountability to international data transfers. A move towards accountability instead of adequacy would mean that a duty of care is placed on all those processing European citizens' data. Steps would have to be taken to demonstrate that the measures in place ensure a level of security based on the risks that data may face when it is being transferred outside the EEA. For example, in the UK, the Information Commissioner already allows data controllers to make their own assessment of whether personal data would be protected once transferred to a given third country.

Clearly, however, it would be important that a move towards accountability in the international context does not simply become an exercise in form-filling to demonstrate compliance.

The Commission should fully examine how accountability can be operationalised to make it an ongoing responsibility and part of the day-to-day operations of data controllers according to the internal governance models of companies in the EU and beyond.

AmCham EU would welcome the opportunity to explore the concept of an accountability-based transfer regime, providing sufficient safeguards and replacing adequacy for international data flows, in more detail with the Commission.

5.2.2 Binding Corporate Rules

Today, Binding Corporate Rules (BCRs) are a way in which some companies, as accountable data controllers, can transfer some data on a global basis outside the EEA.

The Commission has highlighted the role BCRs can play as a self-regulatory solution that enables organisations to demonstrate

their compliance with data protection requirements. On one hand, BCRs are a good example of a current mechanism that can demonstrate accountability while seeking to reduce administrative burdens. Further, they can encourage harmonisation by seeking mutual recognition by authorities. On the other hand, even though BCRs reflect the principle of accountability, they are currently too narrow in scope (e.g. they are limited to intra-group transfers and do not cover data transfers to data processors) and too burdensome for many companies to implement.

It must indeed be recognised that BCRs are a process that requires a great deal of time, resources and money. Securing approval from all EU data protection regulators with jurisdiction over the relevant data transfers can take from 1.5 to 3 years. Many AmCham EU members have not been in a position to make the necessary investment in applying for BCRs and have chosen other tools to enable international data transfers.

Nevertheless, during the past eight years the processes and procedures put in place to facilitate the drafting and obtaining of BCRs approvals have significantly improved; this has improved the ways in which companies can transfer data on a global basis outside the EEA. The fact that a majority of DPAs have acknowledged that this is one of the most viable transfer tools, that a BCR mutual recognition procedure has been introduced and that the time required to obtain approval of BCRs has been reduced are a few examples of the positive developments in relation to the BCRs process over the past years.

The recently built EU BCRs webpage, with an overview of procedures and national requirements, is also a useful tool. There is of course still room for improvement, including having more countries sign up to the mutual recognition system and further simplifying the approval process. It is also imperative that BCRs be added as a separate legal ground for derogation under Article 26 or at least formally recognised as providing adequate safeguards.

AmCham EU believes that, in general, the BCR process can be a useful tool, but calls upon the EU to promote a less burdensome process and a broadening of their scope of application (e.g. not limited to intra-group transfers and coverage of transfers to processors) in order to realise the full potential of this data transfer solution and accountability tool.

5.2.3 Binding Safe Processor Rules

The BCR model is currently mainly used in cases where companies are controllers of the information they process. It does not cover situations where companies are data processors.

AmCham EU would welcome a pragmatic data transfer solution for processors that would be recognised as providing adequate safeguards. We are therefore interested in contributing to and discussing the outcome of the work undertaken with respect to Binding Safe Processor Rules (BSPRs) in the framework of the formal mandate given to the BCR sub-group during a recent A29WP plenary session. AmCham EU believes that, in principle, the idea of an internal governance model for the processing of personal data by multinational companies that would also cover organisations when they act as processors would be worthwhile to explore.

However, AmCham EU would like to caution that BSPRs could only be considered valuable if mechanisms are put into place to avoid the complexity and considerable resources required by the BCR approval process. Otherwise, companies without BCR experience (or without the means to invest the time, resources and money associated with the complex BCR approval process) would be put at a competitive disadvantage.

AmCham EU calls for a flexible internal governance model for data transfers to processors. AmCham EU sees BSPRs as a potentially useful tool in this respect and is ready to contribute to and discuss the outcome of the current work undertaken by European authorities. However, care must be taken to avoid a BSPR procedure that would maintain the complexities and costs associated with today's BCR approval process.

5.2.4 Safe Harbor

The Safe Harbor programme introduced in 2000 has become a widely-used derogation (more than 2,000 certified organisations) for transferring personal data from Europe to Safe Harbor participants in the U.S. Many AmCham EU members have found this a useful tool that provides legal certainty and enables transatlantic business.

AmCham EU members believe that the protection offered to data subjects via Safe Harbor is as robust as that afforded by national data protection enforcement regimes in the EU. Moreover, its

success and popularity have led to a much greater awareness of EU data protection laws in the U.S. It is therefore unfortunate that the process has recently been subject to some ill-informed criticism. The vast majority of the companies that have certified are aware of their responsibilities and have internal or external compliance programs.

Going forward, improvements could be made that would further increase the value of Safe Harbor. One aspect that could be clarified is that data processors established in the US can also certify for Safe Harbor. Data processors' certifications apply the principle of data security, which is something they can control themselves. To comply with the other Safe Harbor principles they require the cooperation of the European data controller (their client). Such a certification by a data processor can be very practical for American IT vendors which receive personal data from their clients located in the EU and need to process it. For this purpose Safe Harbor can be an alternative to entering into Standard Contractual Clauses.

Onward transfer to other (sub)-data processors can be enabled by putting service agreements in place between the data processor that certified for Safe Harbor and its subcontractors that have data protection clauses that at least equal the level of data security as described in the Safe Harbor principles.

AmCham EU would like to see the Safe Harbor programme recognised as a successful tool in this revision.

5.2.5 Standard Contractual Clauses

The Standard Contractual Clauses (SCCs), including one for transfers between data controllers and a recently updated one for transfers from data controllers and data processors, are by now well-known and are used on a wide scale. Many companies have found them useful tools that require less investment than other options, but they are unfortunately not an effective long-term solution to facilitating international data transfers.

An important road block for an even wider use of these SCCs is that many DPAs want to pre-approve every new set of SCCs even when the parties do not deviate from the standard template of the SCCs. This requirement is cumbersome and does not add any practical value. For some countries, it is even unclear whether their DPA requires prior submission or prior approval of new

SCCs. In case such a prior review is requested, the DPAs should act promptly to make a decision. In some countries this process takes several months. AmCham EU recommends the Commission propose a new framework in such a way that no further national review or approval would be required by national DPAs as long as the parties do not deviate from the template text of the SCC.

The utility of Standard Contractual Clauses could be further improved by giving the parties more flexibility to make changes to SCCs as long as the parties to the SCCs remain the same and there are no amendments to clauses made mandatory by the European Commission.

As long as amendments to SCCs are properly signed by the parties, a further review, with its corresponding delay, would not be required.

Finally, currently there is no clear answer as to which type of SCC needs to be used in cases where the data processor is located in the EEA and the client (the data controller) is located in a third country. When personal data is collected in one or more third countries, which may lack a data protection regime or have one that has lower standards than that of the EEA, the conclusion should be that the Directive (and as a consequence the respective national data protection law) does not apply when these data are processed in the EU (in accordance with the instructions of the client) and after processing in the EU are transferred back to the client.

5.3 Universal principles

Universal principles of data protection should be developed to respond to the challenges raised by global data processing. AmCham EU believes that the EU should continue to play a leadership role in working towards a set of universal data protection principles and welcomes the fruitful dialogue established with U.S. authorities regarding data protection.

6 Cooperation and enforcement

6.1 Better cooperation between DPAs and EU authorities

AmCham EU welcomes the work currently being undertaken by the Article 29 Working Party in relation to cooperation between DPAs. It is crucial that DPAs better coordinate their activities and

cooperate more closely, especially with respect to cross-border matters.

AmCham EU also recognises the need for the work of the A29WP to be more transparent. The European Commission could have an oversight and supervisory role in order to ensure consistency and enable mutual recognition wherever possible.

6.2 Harm-based enforcement

The Directive has an insufficient focus on harms and risks and lacks consistent, practical enforcement mechanisms. With the exceptions of some specific provisions, the Directive does not take a harm-based approach or measure degrees of harm to guide consideration of preventative measures, penalties or effective enforcement mechanisms. Taking a harm-based approach may result in better privacy outcomes and is consistent with the human rights approach of the Directive.

AmCham EU believes that enforcement measures are inconsistently applied. Enforcement action should be robust, harmonised and predictable (to the extent possible) and reflect the responsibility of each party. To the extent that one party is processing on the instructions of another party, that other party should be primarily liable in any enforcement action. The parties should be able to contractually allocate risk. If one party is concerned about data protection liability caused by the other, it can seek an indemnity from that other party. To ensure consistency, Member States should adopt a common approach and multiple laws should not apply to the same process. Revenues obtained should be returned to those affected where identification is possible and should not be used to fund the regulator as this distorts the incentive for pursuing sanctions.

AmCham EU believes that formal considerations of harm to data subjects should be a prerequisite for modern legislation as well as for any enforcement action, most notably for imposing fines.

6.3 Class actions

While AmCham EU supports the need to make remedies and sanctions more effective and believes that this can be done by making them more harmonised and predictable. We do not support the introduction of class action procedures, as suggested by the

A29WP document on "The Future of Privacy" as adopted on 1 December 2009, nor the Communication's suggestion [10] of "extending the power of data protection authorities, civil society authorities or other associations to bring an action relating to a number of individuals before the national courts".

AmCham EU cannot support any language that leaves open the possibility of class action suits.

7 Conclusion

AmCham EU looks forward to working with European Union authorities to provide input, expertise and recommendations as the approach to protection of personal data in the EU is reviewed.

* * *

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 US investment in Europe totalled €1.2 trillion in 2008 and currently supports 4.8 million direct jobs in Europe.

* * *

[10] See section 2.1.7, page 9 of the Communication.