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

AmCham EU response to the Commission consultation on protection of personal data

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 number: 5265780509-97
Email: info@amchameu.eu

Secretariat Point of Contact: Christian Borggreen, christian.borggreen@amchameu.eu
Tel: 02 289 10 36

January 19th 2010

Introduction

This document contains the response from the American Chamber of Commerce to the European Union (AmCham EU) to the European Commission consultation on the legal framework for the fundamental right to protection of personal data.

The response is divided into three parts. It starts with a review of the new challenges faced by processing of personal data (Section 1). It then continues with an analysis of both the strengths (Section 2) and the room for improvement (Section 3) of the Directive. As this submission complements the letter AmCham EU sent to Mr. Barrot, Commissioner for Justice, Freedom and Security, on May 18th 2009 regarding some challenges and proposed solutions for EU data protection, a copy of this letter is attached as Annex 1. The letter gives some more detail on concrete issues faced, and possible solutions sought, by AmCham EU members. Annexed is also AmCham EU's Position Paper on International Transfers of Personal Data from December 3rd 2008.

1 New challenges for personal data protection

AmCham EU members list the following as some of the key challenges faced by personal data protection, in particular in the light of new technologies and globalisation:

1.1 Growing complexity and the information age

Globalisation and a networked society have enabled companies to work with customers and suppliers all over the world. Employees, customers and suppliers are now part of a worldwide matrix transcending national boundaries, with growing complexities to be managed. Global data transfers have multiplied exponentially and become by their nature dynamic and multi-directional throughout the world touching many different entities, service providers and data subjects. The European Union (EU) legislative framework largely pre-dates this mega-trend. For instance, the World Wide Web – a truly global and decentralised medium – did not even exist when the Commission proposed the original Data Protection Directive. An increased amount of data is therefore being created, shared, processed and stored across networks and systems that span national, European and international borders. Ensuring the security and privacy of personal data in this environment is key to the future take up and use of online services by the citizens for the benefit of the EU economy. Indeed, the fact that information can be processed more cheaply and at a greater scale than ever before also offers multiple opportunities for society, and is emerging as a key driver for innovation and growth. In addition, new technologies will be able to

provide sustainable solutions to some of the biggest challenges in today's society such as healthcare and climate change. Balancing the protection of the fundamental rights to data protection and privacy with the need to enable economic growth through technology innovation is one of the major challenges in today's digital world.

1.2 Transparency and accountability

In the information age, it has become more difficult to define who should ultimately be held responsible and where to seek redress due to the complex interaction of organisations, data and technologies. More clarity and ownership of responsibility is required at all stages of the personal data lifecycle.

AmCham EU members see technology as a potential solution in supporting both transparency and compliance of privacy policies and keeping the trust of customers and consumers.

The regulatory framework should encourage the development of accountable organisations consistently focused on the protection and rights of individuals and protecting data subjects against actual harms, instead of being focused mainly on processes of regulatory compliance which often add considerable burden and costs while not significantly raising the level of data protection.

1.3 Flexibility, efficiency and trust

The 21st century reality of a true and fast changing digital society spurred by rapid technological innovation requires a flexible framework. The principles-based and technology-neutral approach of the Directive provides a good framework for such a flexible approach and should therefore be maintained. As building and maintaining consumer trust and confidence will be a crucial aspect of technological innovation, the focus of the legal framework should be on the real output in terms of protecting data subjects from harm instead of on producing inputs. Such flexibility is key and should remain while the efficiency should be further enhanced by reducing administrative and legal costs.

2 Strengths of the current Directive

2.1 Introduces harmonisation

The Directive intends to provide a mechanism for harmonisation of data protection laws in the Member States in order to enable the free movement of personal data within the European Union. Harmonisation of data protection laws should contribute to the strength and attractiveness of the European market and create greater efficiencies for both the public and private sectors. While this objective has been met to some extent, there remains much scope to ensure a single market (see below).

2.2 Sound principles and flexible concepts

AmCham EU members consider that the core principles in the Directive - legitimacy, data quality, proportionality, transparency, security and rights for individuals – remain sound. The key concepts of the Directive are flexible and – if appropriately implemented - can cope with the significant advances in technology. These principles can emerge as a leading global paradigm for privacy protection. As an illustration, these principles have been a "starting point" for a number of countries outside of Europe, where many other countries or regions have followed a more risk-based regulatory approach.

2.3 Technological neutrality

The technologically neutral character of the Directive provides a flexible framework which has been able to live up with the technological developments over the years. This approach should remain unchanged. AmCham EU members do not believe that technology-specific regulations and legislation can be flexible enough to be adaptable to new technologies and applications that will emerge in the future. As a result, the Directive should not be amended to refer to specific forms of technology.

2.4 Data subjects' rights

The Directive has served well to help protect users by giving them important and usable rights and has ensured that data privacy is viewed as an important value. The Directive's principles have served as one reference point for good practice for organisations across the globe in terms of developing privacy policies and data subjects' rights.

2.5 Protecting data through its lifecycle

The Directive has been effective in protecting the lifecycle of data from its collection, processing and to its storage and deletion. However, the current legislation does not explicitly address circumstances where data is lost or stolen. Further discussion on this topic needs to take place based on an impact assessment and in consultation with the industry and other interested parties. It should take into account the need of harmonised rules, the risk to personal data and the possible harm to individuals.

3 Room for improvement of the current Directive

3.1 Better harmonisation

Personal data processing are regulated in fragmented ways across the EU today due to differing implementations and/ or interpretations. Each data protection authority has their own interpretation of the broad Directive principles based on their local legal and cultural expectations. While the Directive's broad principles remain relevant and continue to be appropriate it is suggested that a growing lack of legal certainty around how Member States are interpreting fundamental core principles

of the Directive, such as the definition of personal data, is an example of where the Commission's post-consultation review could assist in addressing harmonisation issues and avoid possible legal misunderstanding or non-compliance with the Directive going forward.

The differences in implementation and/or interpretation make it very difficult for businesses to take a European-wide view of data protection compliance. In the knowledge-base economy, this increasingly becomes a significant barrier to the development of the single market. Indeed, when companies handle personal data about their employees, customers and suppliers in various Member States, they are subject to the different implementations, interpretations and applications of the privacy and data protection regimes in force in each EU jurisdiction and they have to deal with different local regulators. The disjointed regulatory approaches create inefficiencies, unnecessary expense and even business barriers for companies seeking to comply with all applicable laws and regulations, without raising the level of protection of data subjects.

The Article 29 Working Party has tried to provide guidance on the application of the Directive on items of Pan-European importance, but its opinions are not consistently followed by national data protection regulators or do not always take into account the economic impact on the single market.

In addition, our members consider that the procedures and output by the Article 29 Working Party need to be more transparent. More openness by establishing regular communication channels with industry and by introducing stakeholder consultations as a standard regime, would produce more workable outcomes and would greatly support efforts towards harmonisation.

AmCham EU members suggest the following steps to be considered and further discussed as part of this consultation by the European Commission:

(i) to provide for enhanced means and resources to enable the European Commission to take further steps towards seeking greater consistency in the application and interpretation of the Directive by consulting with and taking into account the views of data subjects and data controllers as well as seeking input from advisory bodies. To achieve that, AmCham EU believes that there is a need to overcome fragmentation at the policy-making level within the Commission by clearly assigning within the Commission responsibility for the single market objectives of the Data Protection legislative framework;

(ii) look at further enhancing the role of regulatory impact assessments to aid and support a harmonised approach in line with the single market's needs and enable the European Commission to issue guidance to refocus the data protection legal framework on its original single market's goals and avoid that Member States adopt diverging implementation to issues that require a harmonised approach; (iii)

foster a system of mutual recognition among the Member States to

improve key processes at international level and enable a better harmonisation of the Member States' approach, as has been recently the case for binding corporate rules' approval in the context of international data transfers. Pursuant to such mutual recognition procedure, approval by one national regulator would automatically lead to approval by the other national regulators; (iv) consider introducing a "country of origin" principle as implemented for e-commerce and financial services making it possible to apply the lead authority concept defined for the binding corporate rules to data protection compliance generally. Such approach could indeed enable companies to concentrate their compliance efforts in a consistent and effective way with one regulator. This would save enormous resources to businesses operating cross borders and should e.g. apply for the data security measures of an EU data controller. When the data collection by one company takes place in various EU Member States, often with the involvement of its European affiliates, the data security measures to apply should be those of the country where the head office is established. In the current framework, such a company which may outsource the data processing to a service provider, may have to comply with all national data security requirements applicable in each country where the data collection takes place.

We would like to emphasise that a greater harmonisation does not necessarily require a change of the existing provisions but rather the identification of the available means to ensure consistent interpretation across the EU Member States.

3.2 Definitions under the Data Protection Directive 95/46 EC

There continues to be a lack of legal clarity and harmonisation with respect to definitions of a number of fundamental data protection concepts such as "personal data", "data controller/ data processor", "co-controller" and "consent". This creates substantial uncertainty for both data controllers and data subjects and it needs to be addressed. AmCham EU members have elaborated in some detail on these issues in the letter to Commissioner Barrot (see Annex I). The main points can be summarised as follows.

Significant legal uncertainty has arisen around the processing of data, which still may be linked to an individual but not by the party processing the data. For example, in some Member States key coded information (e.g. in pharmaceutical tests) is in some cases still considered personal data even if the key codes are not held by the data controller and there is no realistic chance it could obtain them. Another concern is the definition of IP addresses and whether a website provider should treat them as personal data.

The concept of personal data should be defined following the so-called relative approach, where data is considered personal for someone who can link the data to identified individuals. Getting the response right to

the question of where to draw the boundaries of "personal" data is fundamental to the success of Europe's knowledge society. Modern R&D fuelling new businesses and solutions generally relies on the analysis of aggregate information, where it is critical to disambiguate individuals from each other in an anonymous fashion. With this view, having the definition of personal data in mind as meaning any information relating to an identified or identifiable natural person, information should only be considered to relate to an "identifiable" natural person when it is likely to be linked to identified individuals taking into consideration the time and manpower that would be required as well as the purposefulness of identifying an individual in the frame of an organisation's lawful activities. The mere possibility of identification (for example through cross-reference of the available information with other third party sources) should not be sufficient to meet the threshold of the definition. There needs to be a degree of reasonableness and a proximity link between the information available and the identification of the individual in question.

Another major concern of AmCham EU members is the lack of clarity around the terms "controller" and "processor". Parties acting in similar capacities are not qualified in the same way throughout the Member States. Moreover, the definitions of these central concepts do not reflect the reality of the complex control relationships that govern the handling of personal information in today's world, creating confusion and unnecessary obstacles to the legitimate processing of personal data. It is legitimate to consider whether the distinction between "controller" and "processor" should be abandoned in favour of a flexible approach where each party that processes personal data is responsible based on its own role in the data processing.

3.3 Less bureaucracy

The formalities of rules as imposed by the Directive result in significant compliance costs and result in unequal enforcement. In particular, registration and notification requirements and processes are often unclear in terms of applicability, and create unnecessary processes, which vary between Member States.

Some Member States only require that the data controller registers its company with the national regulator (e.g. the UK), while others Member States (e.g. Belgium) require that each processing serving a different purpose must be notified. In other countries (e.g. Germany), the data controller can register its internal data protection officer with the national data protection regulator and in such a case the notification of new systems that process personal data will only be done to this person. Additionally, each data protection authority requires their own forms to be completed and poses distinct questions reflecting their own individual concerns. The situation becomes more complex where different forms are required to be completed for different data files. For certain forms, organisations are required to provide substantial details

about the type of processing undertaken. As a result an organisation operating across the EU must file separate registrations in each jurisdiction where it operates as a data controller taking account of all the local requirements and peculiarities, without benefiting from economies of scale. This generates a considerable degree of bureaucracy and costs, which can amount to several thousand euros for each jurisdiction just to understand what information is required for the form and to complete it. Furthermore, the amount of detail required for a filing can mean that the filings frequently need to be updated to ensure that they are still current.

Some Member States have in place simplified notification regimes (e.g. France), and some others even have exemptions to the notification obligation under specific circumstances (e.g. the Netherlands and Belgium exempts many standard systems for data processing).

The European Commission should conduct an analysis into the rationale and benefit of the registration's and notification's obligations and re-assess the need to impose such obligations upon data controllers. It is only in case the conclusion would be that such notification would considerably enhance the way personal data are processed in the EU that this requirement should remain in place. However, in that scenario the European Commission should develop a common template for (electronic) notification of data controllers to be accepted by each EU Member State.

Indeed, AmCham EU members consider that the traditional justifications for notification (i.e. prior checking of data controllers and their processing operations, providing data subjects with information, funding the national data protection authority) should be balanced with the heavy burden for data controllers of complying with such diverging obligations across Member States. The different approaches to notification create real compliance difficulties when trying to operate on a pan-European basis and are a barrier to the establishment of a single market. AmCham EU members therefore see a strong case for abolishing or considerably easing the notification requirements to high-risk scenarios and/or ensuring that they are applied on a more uniform basis across the EU.

For cases where notifications is deemed necessary, the European Commission should consider a notification procedure consistent across all Member States with mutual recognition so as to avoid unnecessary duplication of formalities to cover all of an organisation's operations in the EU. The exemption system should be streamlined, non-registration should be the general rule; notification the exception, and only where high-risk processing occurs and when transparency cannot be ensured by other means. Any remaining notification process should be pragmatic and light. The content of these notifications should be limited to key information, to limit the need for time and cost-consuming updating.

AmCham EU members would favor a notification of data controllers as opposed to registration of databases or data processing operations.

AmCham EU members also support better use of the possible exception offered in the Directive[1] via the appointment of a data protection officer as an adequate global and voluntary alternative to notification duties, at least with regard to certain industry sectors. It may indeed be an important item of simplification for data protection authorities not to have to deal with the review of massive numbers of notifications filed and it provides a relevant independent expertise and oversight by a person who should know the business of the data controller well. At the same time, this would be a great opportunity for national data protection regulators to devote the necessary resources to working with these officers in achieving a more accountable system instead of focusing on ex-ante inputs.

3.4 International data transfers

The need to facilitate international data transfers is imperative for business today in a global economy. International data transfers have grown in complexity with globalisation and the evolution of technology, but the EU privacy regime has been lacking a practical mechanism for compliance. Transfers of personal data should be able to take place without the need for complex, lengthy and costly processes when there are adequate protections in place within accountable organisations. AmCham EU has throughout the past years been heavily involved in a global search for workable data transfer solutions. We refer in that respect to our last Position Paper on International Transfers of Personal Data issues on December 3rd 2008 which we also enclosed for your convenience (see Annex II).

We summarise below the key data transfer issues identified by AmCham EU members:

The current system for assessing third countries is burdensome and time-consuming. Rather than the current scheme which automatically excludes countries outside the EEA and requires their assessment, which means in fact a test of equivalence of their local system with the Directive, the European Commission should allow transfer of personal data to countries outside the EEA that have democratic systems and a rule of law that would allow individuals to seek legal redress in case of misuse of their personal data by a data controller or data processor located in any of such countries.

With the exception of Safe Harbor for data transfers to the United States, for many data transfers, standard contractual clauses adopted by the European Commission are the only practical solution. The use of these standard contractual clauses raises a number of issues

[1] Art. 18.2 Data Protection Directive.

that are primarily due to the fact that they have not been drafted for global businesses transferring data all around the world but rather for much easier situations involving two parties only. This means that their implementation often requires amendments to allow their use in a global context. The local procedural requirements still vary considerably from one Member State to another. The large majority of the Member States impose formalities of filing or approval with very little flexibility often imposing the use of the exact mirror of the standard clauses adopted by the European Commission. In addition, the level of detail required in the schedules of the standard contractual clauses also varies significantly among Member States. Some regulators require only a general overview of the types of data transferred, whereas others require detailed information about these data flows. More harmonisation on these points is crucial to ensure a smooth and efficient use of the standard contractual clauses as an effective reference for data transfers.

Although some significant steps have been taken to favour binding corporate rules ("BCRs"), the BCR process could be more transparent and streamlined and improvements are still required to enable them to fully take off as one of the most appropriate solutions for multinational businesses. Such improvements include (i) ensuring that all data protection regulators are in a position to recognise BCRs subject to local law requirements, (ii) ensuring more transparency regarding national procedures and requirements (including access to precedents), (iii) extending mutual recognition to all regulators in the thirty EEA Member States, (iv) ensuring a sufficient publicity of the existing approved binding corporate rules with a view to making them a recognised and global solution for data transfers and (v) not making BCRs subject to overly onerous national procedural requirements. Finally, the existing mutual recognition system for the approval of BCRs should be enhanced so that BCRs can be used for transfers to data processors located outside the EEA.

AmCham EU members also call upon the European Commission to publish on its website a list of the national requirements applicable both to standard contractual clauses and BCRs. Such list would facilitate data controllers' compliance and identify Member States which would have gone beyond the requirements of the European Commission in their implementation of the Commission's decisions.

As a result, the strict rules governing transborder flows of personal data should be re-visited with a more global mindset allowing a flexible approach in the application of the exceptions to the principle of prohibition.

3.5 Harm, risk and enforcement

The Directive has 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 harms-based

approach, or measure degrees of harm to guide consideration of preventative measures, penalties and effective enforcement mechanisms.

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

Taking a harms-based approach may result in better privacy outcomes and is not inconsistent with the human rights approach of the Directive. Criteria for better determining risk involved in data processing should include issues such as scale of processing, sensitivity of data and field of activity of data controller to help define a risk-based approach. This would not only provide greater comfort to data controllers in deciding how to operate their business and how to ensure that the appropriate technical and organisational measures have been put in place to ensure data security and privacy but would also focus attention on substantive data protection issues at board level and away from minor technical breaches.

On the enforcement side, AmCham EU considers that enforcement measures are inconsistent in their application and possible liabilities are not always clearly published.

Enforcement action should be robust, (to the extent possible) harmonised and predictable 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 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.

* * *

ANNEX 1

AmCham EU letter to Commissioner Barrot regarding the main challenges and proposed solutions for EU data privacy, 18 May 2009

ANNEX II

AmCham EU Position Paper on International Transfers of Personal Data, 3 December 2008

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE
TO THE EUROPEAN UNION

Avenue des Arts/Kunstlaan 53, B- 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
Email: amchameu@amchameu.be
www.amchameu.be

May 18th 2009

Mr. Jacques Barrot
European Commission
Commissioner for Justice, Freedom and Security
1049 Brussels

Dear Commissioner Barrot,

As a follow-up to our meeting last year with your Cabinet and in view of the May 19th-20th 2009 Data Protection Conference organised by the European Commission in Brussels, the American Chamber of Commerce to the European Union (AmCham EU) is pleased to provide you with our thoughts regarding the main challenges and proposed solutions for EU data privacy. We furthermore present you with specific issues our members are facing in practice which we would like to see addressed by the Commission. We would be delighted to explain these in more detail at another time.

We would like to note that we do not specifically address all issues related to the current discussion on the possible revision of the EU Data Protection Directive 95/46/EC ('Data Protection Directive') in this letter, in particular with respect to the need for including the use of new technologies within its scope. AmCham EU members may follow-up with specific comments in this respect and would welcome the opportunity to discuss the application of the existing legislation in relation to Radio Frequency Identification (RFID) technologies, the enabling technologies of the so-called Internet of Things (IoT), as well as issues related to the use of profiling techniques, behavioural advertising and social networking.

The main point AmCham EU members would like to raise in this letter, is the lack of consistency amongst national data protection laws in the EU, which continues to remain one of the most serious hardships. Indeed, divergent styles of implementation at the local level make compliance by international businesses very challenging, and is often at odds with producing and implementing coherent multi-jurisdictional privacy policies and compliance programmes, especially for multinationals with establishments or operations in several EU Member States. Some examples of the lack of harmonisation are provided below.

Definitions under the Data Protection Directive 95/46 EC

Personal data/Anonymized data
In general, most Member States' definition of personal data is consistent with the Data Protection Directive and the broad interpretation of the Article 29 Working Party ('WP29') as contained in its Opinion on Personal Data released in June 2007.
However, there are still variations in the interpretation of the definition between Member States which may lead to practical complications for data controllers

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE
TO THE EUROPEAN UNION

Avenue des Arts/Kunstlaan 53, B- 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
Email: amchameu@amchameu.be
www.amchameu.be

operating in multiple jurisdictions. Indeed, the Commission already spotted this in the technical analysis of the transposition in the Member States supporting the Report on the First Report on the implementation of the Data Protection Directive, "*there appears to be division among Member States on whether or not to use a relative approach to the concept of personal data in the sense that data are considered personal for someone who can link the data to identified individuals*".

In this respect, our members face issues when processing data, which, still can be linked to an individual, but they are not themselves able to make that link. Rather than considering such a merely theoretical possibility to be sufficient, our members would support a more risk-based approach, requiring the person who processes the data to also have access to the link in order for that data to be considered personal data.

The interpretation of what should be considered anonymized data is also dealt with differently from one Member State to another. As an example, some Member States consider information as 'personal data' if anyone holds the information (e.g., a key) necessary to identify the relevant individual. This is the case regardless of whether or not the data controller is likely to ever obtain the information necessary to identify the relevant individual from the relevant third party. For example, in some Member States key coded information is in some cases still considered personal data even if the key codes are not held by the data controller and there is no realistic chance it could obtain them. Another concern is the definition of IP addresses and to what extent the IP address is actually considered personal data. The level of re-identification of the data should be taken more into account with regard to the compliance obligations imposed on such data.

One possibility to deal with these aspects could be to introduce a harmonised definition of indirect or pseudonymous personal data that could benefit from lighter data protection requirements as the processing of such type of data usually present very low risks to privacy.

Controller/ Processor

One of the major concerns of AmCham EU members is the lack of clarity around the terms "controller" and "processor:" Parties acting in similar capacities are not qualified in the same way throughout the Member States. In some Member States it is fine for a processor to have a certain degree of discretion especially as regards the means of the processing, whereas in other Member States such discretion would render him a controller.

This uncertainty has been of particular concern in the outsourcing context. One of the main purposes of any outsourcing is that the outsourcing company suggests and puts in place a new way of improving its working process or a solution, often consisting of pre-set modules, software and/or hardware. This should, however, not *per se* bring the local data protection authority to the conclusion that the outsourcing company decides on the purposes and means of the processing and therefore be considered a data controller.

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE
TO THE EUROPEAN UNION

Avenue des Arts/Kunstlaan 53, B- 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
Email: amchameu@amchameu.be
www.amchameu.be

It is essential that outsourcing and other service providers established and operating in Europe are not put in a position of competitive disadvantage vis-à-vis those service providers that operate in third countries, such as India, Philippines, China, because they have additional data protection compliance burdens or legal uncertainties across Europe in respect of their role and related obligations.

The definitions of "controller" and "processor" are not easy to distinguish between in practice as they contain concepts that may overlap, i.e., an entity determining the purposes and the means of a processing, as a controller would do, may at the same time act upon instructions and on behalf of another company, as a processor would do.

The granularity of the elements to be taken into account when determining whether a person acts as a processor or controller should be clarified and clear guidelines should be provided on how to decide whether their responsibilities fall within those of a data controller or of data processor. The current definitions are too static and are not adequately applied to entities involved in the modern networked economy, where service providers often offer solutions/packages.

Co-controllers
The definition and the legal implications of the "co-controller" concept should also be interpreted in a more harmonised way. It is unclear under which scenarios there are co-controllers. Often one party determines the means and the other the purposes of the processing, and therefore the interpretation of a joint determination may prove difficult in practice. AmCham EU members also consider that such a concept should allow for an allocation of the obligations between data controllers without providing for joint and several liabilities between them.

Consent
There is also a lack of harmonisation between Member States regarding the definition of freely given informed consent. Certain Member States indicate that employees are generally not able to provide free consent, whereas others always require consent for the processing of certain categories of data (e.g., sensitive data). We call upon recognition of "consent" as a valid legal ground for the processing in each case where such consent is in favour of the data subjects. Consent should not be required, where the processing can be justified on other legitimate grounds.

Some Member States require written consent in most cases. We also consider that appropriate technical solutions exist to collect data subjects' unambiguous consent and these applications should not be disregarded.

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE
TO THE EUROPEAN UNION

Avenue des Arts/Kunstlaan 53, B- 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
Email: amchameu@amchameu.be
www.amchameu.be

Extraterritorial application and competition impact

AmCham EU members' experience shows that the extraterritorial application of the Data Protection Directive may have a major impact on EU business, especially when it comes to competition.

For example, if a US-based company intends to outsource the processing of data abroad (e.g., management of its global customer database), it will think twice before choosing to outsource to an EU-based firm as this could lead the US-based company to become a data controller subject to the rules of the Data Protection Directive (which would never be the case if it chooses a non-EU based processor). Indeed, some Member States interpret article 4(c) of the Data Protection Directive to mean that the data protection law of the Member State where the processor is located applies: *"(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community*". If the processor is using equipment which is not only used for transit, the parties would have to comply with the local data protection rules of the Member State where the processor is located.

Such a situation could, for instance, lead to having customer data, freely received by the data processor in one EU Member State, to no longer be freely re-exported to the US-based company, after processing. The parties would have to seek a derogation based on article 26 of the Data Protection Directive for returning personal data received in the EU to the US.

Registration with national Data Protection Authorities

Various registration regimes and exemptions
AmCham EU calls for a more harmonised registration regime of the processing activities to the national data protection authorities as registration requirements and procedures may prove very formalistic and burdensome for businesses operating in various EU Member States. Currently each Member State has different registration processes and the exemptions to the registration obligation vary from one Member State to another.

The WP 29 also recognised this issue in its Opinion on the obligation to notify the national data protection authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union released in January 2005 (WP 106 Opinion) : "*Data Protection authorities within the Article 29 Working Party agree on the need to streamlining the exemption system by inviting the Member States where some exemptions are not provided for to consider possible harmonisation attempts. It would be desirable that data controllers could benefit from the same catalogue of exceptions and simplification everywhere in the European Union*".

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE
TO THE EUROPEAN UNION

Avenue des Arts/Kunstlaan 53, B- 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
Email: amchameu@amchameu.be
www.amchameu.be

Any harmonised approach should envisage non-registration as the general rule and registration as the exception only where high risk processing occurs and when transparency cannot be ensured by other means. Any remaining registration process should be pragmatic and light. Member States should be requested to modify their national laws accordingly. In that respect, AmCham EU members would favour a registration of data controllers as opposed to registration of databases or data processing operations.

Data Protection Officer

The establishment of data protection officers may be an important item of simplification for data controllers (but also for data protection authorities whose work could therefore be focused on certain data processing or sectors more likely to be prejudicial for the privacy of individuals) without reducing the information accessible for the data protection authorities.

In its WP 106 Opinion, the WP29 indicates that generalising this solution "*would be useful in view of the positive findings reported by the Member States in which these data protection officials have been already introduced or have existed traditionally*".

Our members support the appointment of data protection officers as a substitute to notifications duties, at least with regard to certain industry sectors. However, as was underlined by the WP29, this possibility is still not available in most countries.

Simplified registration or exemption for employee data

AmCham EU recognises the value of publicly registering data processing operations that may present a risk to privacy. However, certain types of processing operations do not benefit from public registration as other more direct ways to obtain the relevant information is available to data subjects. For example, employees will normally ask their employers' human resources department for any details regarding the processing of their data.

AmCham EU members support the WP 29 idea developed in its WP 106 Opinion mentioned above regarding the necessity to streamline the exemption system among the Member States' legislations. Such a harmonisation process should at least concern the processing of data that are already subject to exemptions *lato sensu* under the Data Protection Directive, e.g., processing required to comply with existing legislation, in particular as regards data in the employment sector.

Notification and approval of international data transfers

The overall scheme of notifying data transfers to DPAs and, where required, getting their approval prior to a transfer is very bureaucratic and burdensome and does not provide increased protection to data subjects when Standard Contractual Clauses are used. In practice, many DPAs are not responsive to transfer requests, resulting in unreasonable delays of an approval in some jurisdictions, sometimes more than a year.

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE
TO THE EUROPEAN UNION

Avenue des Arts/Kunstlaan 53, B- 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
Email: amchameu@amchameu.be
www.amchameu.be

We support any initiative that would shorten the length of time and effort required to get data transfer clearance and approval. In particular, there should be no approval requirement for transfers where Standard Contractual Clauses or Binding Corporate Rules are used. We also call upon the Commission to put in place electronic and centralised filings as this could play an important role in removing part of the complexity of complying with transfer requirements. Coordination between Member States should also be increased in this area.

International data transfer issues

We would welcome the rules on international transfers to be reconsidered in the current time of globalisation and "cloud computing" as most of the solutions in place are not adequate for an increasingly global environment. AmCham EU has throughout the past years been heavily involved in a global search for workable data transfer solutions. We refer in that respect to our last Position Paper on International Transfers of Personal Data issued on December 3rd 2008 which is attached for your convenience.

Extension of "white list" of third countries
AmCham EU member companies urge the Commission to review its adequacy finding process in order to allow more countries with data protection rules in place to be recognised as ensuring an adequate level of protection of personal data. The current system for assessing third countries seems too burdensome and lengthy. Our understanding is that it verifies more the equivalence of the local system with the Data Protection Directive than the adequacies as such of the local rules, without taking into account the local data protection realities and efforts.

National requirements when using Standard Contractual Clauses
AmCham EU members call upon Member States to apply uniform procedural requirements when the Standard Contractual Clauses are used. The procedural requirements still vary a lot from one Member State to another: some Member States require data controllers to file these Standard Contractual Clauses, while others still require even approval of the transfer.

In the short term, our members would welcome a summary from the Commission on the local requirements regarding the use of Standard Contractual Clauses in each Member State as it is currently the most common tool used for transferring personal data outside of the EU. In the long term, our members would welcome a clarification that data controllers would only have to deposit one copy of the Standard Contractual Clauses in a central repository for transparency purposes without the need for approval.

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE
TO THE EUROPEAN UNION

Avenue des Arts/Kunstlaan 53, B- 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
Email: amchameu@amchameu.be
www.amchameu.be

Multi-party and multi-purposes data transfer agreements

As was already proposed on the occasion of the Conferences on Cross-Border Data Flows jointly organised by the US Department of Commerce, the EU Commission and the Article 29 Working Party in 2007 and 2008, AmCham EU welcomes the proposal for an express extension of the use of Standard Contractual Clauses in a multi-party context and/or multi-purpose context and would be happy to assist in proposing appropriate wording. This will facilitate the use of the Standard Contractual Clauses for multi-party and/or multi-purposes transfers of personal data.

Simplified procedure for intra group data transfer agreements

We would like to see a distinction in approach between intra-group and external data transfers. Indeed, our members who are mainly multi-national organisations operating across boundaries apply the same high standards of data protection across all jurisdictions where they are present, which could justify a lighter set of data transfer clauses to be used for intra-group transfers as opposed to transfers of personal data to persons outside the group.

Reviewed Controller-to-Processor Clauses

AmCham EU was, together with other trade associations very much involved in the preparation of a new set of Standard Contractual Clauses for data transfer to processors in third countries, which would allow sub-processing by the processor.

We welcome the WP 29 Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries as it is a step in the right direction but we remain concerned about some of the main issues covered in the draft we suggested do not seem to have been taken into account. We would therefore welcome an opportunity to explain our point of view before a final Decision is adopted by the Commission.

Binding Corporate Rules

AmCham EU member companies are pioneering the use of Binding Corporate Rules (BCR) as an alternative to other derogations allowing for international data transfers. However, it has proven difficult to receive approval of these rules from the relevant authorities and this within a foreseeable period of time. In addition, while the Commission's Communication on better implementation of the Data Protection Directive highlights work done so far with respect to international data transfers, it also recognises the need for continued efforts and improvement in this field. Some required improvements are: ensuring all Data Protection Authorities ('DPAs') are able to recognise BCRs, which may require a change in national laws; ensuring more transparency regarding the additional national DPA requirements for BCR approval; extending the mutual recognition of a lead DPA's approval by all DPAs; and not making BCRs subject to overly onerous national procedural requirements.

The Commission should encourage further simplification in the area of international data transfers by innovative and streamlined mechanisms, such as BCRs and reviewed Controller to Processor Contractual Clauses. BCRs are a particular example of how a

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE
TO THE EUROPEAN UNION

Avenue des Arts/Kunstlaan 53, B- 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
Email: amchameu@amchameu.be
www.amchameu.be

multinational company can demonstrate and ensure data privacy accountability. BCRs provide for real solutions, as they deliver real compliance and real benefits for the individuals, whilst allowing companies to benefit from global data flows. BCR approach should be further extended and adapted for the use by service providers (data processors) in respect of data they process on behalf of the clients (data controllers).

Sector-specific data transfer solutions
We would also support any development of sector-specific data transfer solutions which could include specific annexes and/or policies to cover the usual transfer of data taking place within a specific sector of activities (e.g., pharmaceutical and financial services).

Finally, in today's global information society and emerging new technologies and services that rely heavily on international flows of data, the current complex rules for international data transfers in the EU may result in a competitive disadvantage for companies established and operating in Europe. These companies, in particular in technology and information services sector, are subject to additional requirements, costs and delays, with the effect that they may loose a battle against increasingly fierce competitors in third countries, who are not subject to the same rules.

Support for global privacy standards, Privacy Enhancing Technologies and privacy by design

AmCham EU welcomes the setting up of global privacy standards that would enable companies to certify that they have in place adequate privacy compliance measures and would be happy to participate in the setting up of any such standards, if you deem it appropriate. Such standards should set out certain principles and remain technology-neutral.

We see technology as instrumental in supporting compliance of privacy policies and recognise the need to ensure that as information systems that hold personal information and accompanying procedures are developed, privacy concerns are identified and addressed from the beginning.

Conclusion

Full harmonisation of legislation at the EU and even at a global level would be the ideal solution whereby data would flow freely under a standard regime. However every step towards establishing a common denominator of standards for processing and transferring data as described above, would help businesses significantly.

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE
TO THE EUROPEAN UNION

Avenue des Arts/Kunstlaan 53, B- 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
Email: amchameu@amchameu.be
www.amchameu.be

In our view, it is essential to reduce the massive requirements for business imposed by differing implementation of the Data Protection Directive in the 27 EU Member States. Therefore, we welcome any efforts to interpret and build upon the already existing exceptions under the Data Protection Directive to further improve the management of personal data in an international context.

AmCham EU is deeply committed to a close dialogue with relevant authorities to advance these issues and is looking forward to ongoing collaboration.

We hope very much that the information provided above will assist you in your work on this dossier and will help to ensure that the final outcome offers a workable and balanced approach that is in the interests of both companies and individuals' privacy.

We look forward to working with you further on these issues and in the meantime we remain at your disposal for any further information which you may require.

Yours Sincerely,

John Vassallo
Chair, American Chamber of Commerce to the European Union

Karim Lesina
Chair, Digital Economy Committee, American Chamber of Commerce to the European Union

* * *

AmCham EU is the voice of companies of American parentage 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 play a role in creating better understanding of EU & US positions on business matters. Total US investment in Europe amounts to $702 billion, and currently supports over 4.1 million jobs.

* * *

AMCHAM EU
AMERICAN CHAMBER OF COMMERCE
TO THE EUROPEAN UNION

Avenue des Arts/Kunstlaan 53, B- 1000 Brussels, Belgium
Telephone 32-2-513 68 92 Fax 32-2-513 79 28
E-mail: amchameu@amchameu.be

December 3rd 2008

Position Paper on International Transfers of Personal Data

Executive Summary

- Workable solutions for international transfers of personal data are essential for businesses operating on a global scale. The excessive requirements imposed on business by 27 differing national data protection regimes must be reduced by ensuring a consistent implementation in the EU member states.

- The exceptions under Art. 26 of the directive constitute a workable alternative to regulate the transfer of personal data to "non-adequate" third countries. AmCham EU is keen on working together with authorities to find workable solutions which should be consistently applied throughout the EU.

- In particular, AmCham EU champions the use of Consent, Standard Contractual Clauses, Binding Corporate Rules ('BCRs') and Commission Adequacy Decisions to manage international employee, customer and consumer data.

Subject	Business Perspective	AmCham EU Position
General assessment	Flexible mechanisms for international data transfers are key for companies operating on both sides of the Atlantic.	The EU Data Protection Directive needs to be implemented consistently in all 27 EU member states. The use of the exceptions under Art. 26 should be further facilitated.
Binding Corporate Rules (BCRs)	BCRs provide a promising mechanism for companies to transfer data to non-EEA countries. The benefit is a unified, global company standard, tailored to a company's unique culture or business compliance processes.	The BCR approval process should be improved by: ensuring all Data Protection Authorities ('DPAs') are able to recognise BCRs; ensuring more transparency regarding the additional national DPA requirements for BCR approval; extending the mutual recognition of a lead DPA's approval by more DPAs; and not making BCRs subject to overly onerous national procedural requirements.

Standard Contractual Clauses	Alternative Standard Contractual Clauses are a valuable means to legitimise data transfer outside the European Economic Area ('EEA'). However, a number of practical difficulties remain in the application of the clauses.	EU member states should apply uniform procedural requirements when using the clauses. Onward transfer to a data processor should be allowed. In addition, the use of Standard Contractual Clauses should be extended in a multi party-context.
Consent	Consent is a useful tool for transferring personal data to third countries, in particular relating to employee data for specific applications. Adequate prior information needs to be provided.	Consent, based on an appropriate notice, must remain acceptable as a valid legal basis for the international transfer of personal data for specific purposes such as HR management. The legal requirements should not go beyond what is asked for in the EU 95/46 Directive.
Safe Harbour	The Safe Harbour Agreement is a success, as it provides a flexible and well-structured process to manage the free flow of information between signatories of the agreement.	AmCham EU strongly supports the Safe Harbour agreement. It should be extended to those sectors of financial services and telecommunications currently excluded.

Introduction

The American Chamber of Commerce to the European Union (AmCham EU) issued a joint press release with the International Chamber of Commerce (ICC) on October 23rd 2006, calling upon decision-makers on both sides of the Atlantic to deliver real progress on more flexible mechanisms for international transfers of personal data. This position paper is a follow-up to that press release and provides recommendations on the various exceptions for international transfers of personal data under the EU Data Protection Directive (95/46/EC), ("the directive").

Global businesses are increasingly faced with the daunting challenge of managing the growing complexities of their employee, customer and other personal data. Globalisation and a networked society have enabled companies to work with customers all over the world and employees are now part of a worldwide organisational matrix transcending national boundaries.

The directive imposes significant barriers to international data flows by generally prohibiting the transfer of personal data to countries located outside the EU/EEA[1] that are deemed not to provide adequate data protection. For the time being, the EU only

[1] EEA (European Economic Area) consists of the EU 27 plus Iceland, Liechtenstein, and Norway

considers Argentina, Canada, Guernsey, the Isle of Man, Jersey and Switzerland as providing adequate protection.

Accordingly, if a company wants to transfer personal data to a "non-adequate" country, it needs to comply with one of the exceptions under the directive (Article 26). These exceptions include, for instance, Binding Corporate Rules, Standard Contractual Clauses, Consent and other types of available instruments, e.g. the EU-US Safe Harbour Agreement.

Yet the EU legal framework has not effectively supplanted national decision-making mechanisms forcing companies to comply with rules from 27 different regimes when transferring data. Companies operating outside the EU, notably in the US, are especially hard-hit by this massive set of requirements. Therefore, AmCham EU has been involved in a global search for workable solutions.

We recognise the vital role of the EU-US Safe Harbour Agreement which lays out seven principles on data privacy. AmCham EU has cooperated with other business organisations to draft alternative Standard Contractual Clauses for data transfers between controllers, approved at the end of 2004 by the European Commission ("the Commission") and the Data Protection Authorities (DPAs). Another set of alternative Standard Contractual Clauses between controllers and processors, to which AmCham EU also contributed and which has received positive feedback from the Commission, is being evaluated by the Article 29 Working Party.[2] We are hopeful that these Clauses will be formally approved in the near future.

AmCham EU member companies are also pioneering the use of Binding Corporate Rules as an alternative to other derogations allowing for international data transfers. However, it has proven difficult to receive approval of these rules from the relevant authorities. In addition, while the Commission's recent Communication on better implementation of the directive highlights work done so far with respect to international data transfers, it also recognises the need for continued efforts and improvement in this field.[3]

The remainder of this paper will discuss these exceptions under Article 26 of the directive in more detail and provide recommendations to further improve the management of personal data in an international context.

[2] Advisory body composed of representatives of the national data protection authorities, the European Data Protection Supervisor and the European Commission.
[3] Communication on the follow-up of the Work Program for better implementation of the Data Protection Directive (COM (2007) 87 final); Adopted on March 7th, 2007.

Binding Corporate Rules (BCRs)

In 2003, the Article 29 Working Party, in consultation with the Commission and following various meetings with stakeholders issued a working document (WP 74) on Binding Corporate Rules (BCRs).[4] The document states that the EU is favourably disposed to the idea that multinational companies should be able to establish a global privacy policy, the so-called Binding Corporate Rules, to enable cross-border transfer of personal data between their group companies in accordance with European data protection requirements.

BCRs allow for a unified, global company standard. They are an in-house policy, driven by and tailored to a company's unique culture or business and compliance processes, and improve a company's ability to communicate rules and values to employees, customers and consumers. However, in order to make this alternative truly viable, DPAs need to improve their approval process and, in many instances, recognise the very concept of BCRs.

Some AmCham EU member companies had already, prior to the WP 74, contemplated BCRs as an alternative to transferring data and had sought individual DPA approval of their BCRs. However, that process proved very time-consuming for both the companies and the DPAs involved. Thus, AmCham EU members very much welcomed the Commission's and the Article 29 WP's efforts to formalise the approach and agree upon a coordinated approval process of BCRs. The coordinated approval process allows for a simplified procedure for BCRs and in theory, should mean fewer unique data processing approvals for the DPAs. The WP 74 also, to some extent, increased and clarified the role for DPAs in enforcing and approving BCRs of global companies.

The adoption of the Article 29 WP working document (WP 108)[5] of a model checklist application for approval of BCRs was another step toward improving the BCR approval process. The checklist provides a set of questions that a company can use when submitting an application to have its BCRs approved by a local DPA within the EU. The checklist also sets out the procedure for companies to follow to ensure that their BCRs are approved by all relevant DPAs and gives guidance as to which DPAs a company should submit their BCRs to for approval.

[4] WP 74 Working Document: Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers; Adopted on June 3rd, 2003.
[5] WP 108 Working Document: Establishing a Model Checklist Application for Approval of Binding Corporate Rules; Adopted on April 14, 2005.

AmCham EU also very much welcomes the adoption of a standard application form for the approval of BCRs (WP 133)[6], together with the framework (WP154)[7] and FAQs (WP 155)[8] for BCRs. This should make the initial BCR application easier. Before these documents were introduced, each DPA has had its own application form or, alternatively, has not had one at all.

The BCR approval process has come a long way in a few years' time. However, significant problems remain. The time consuming and costly nature of the application process, together with the onerous obligations imposed under BCRs, mean that many organisations, including existing applicants, are actively questioning their use as a compliance strategy. AmCham EU therefore calls upon the Commission and the DPAs to seriously consider the issues raised below and attempt to address them in an expedient manner.

Recognition of BCRs

A number of DPAs do not believe they have the discretion to approve BCRs under their national laws. For example, the Italian Garante has invited Parliament to amend the Consolidation Act regarding the *Protection of Personal Data (Data Protection Code - Legislative Decree No. 196 of June 30 2003)* to allow it to approve BCRs in Italy. Similarly, the Belgian Commission for the Protection of Privacy requires a Royal Decree to be passed to approve the use of BCRs in Belgium. If BCRs are to be seen as a credible compliance strategy then it is vital that they are available in all Member States. AmCham EU calls on the Commission and all DPAs to ensure they are able to recognise BCRs.

Resources and transparency

A major obstacle with the BCR approval process is the lack of dedicated resources within the various DPAs. Despite attempts to streamline the process, the BCR process is still complex, lengthy and costly for the applicant and DPAs seldom have enough dedicated resources to deal with them. Typically, the DPAs do not have the capacity to handle more than a dozen or so applications per year. In addition, potential applicants are still deterred by the lack of information about which DPAs accept BCRs and the DPAs' additional national requirements on top of the standard application form. AmCham EU members call upon DPAs to allocate more staff in order to handle this issue effectively. AmCham EU also asks that the Article 29 Working Party establish a webpage to ensure more transparency regarding the use of BCRs such as a list of the DPAs which accept BCRs and a list of each DPA's specific national requirements in order to approve a company's set of BCRs.

[6] WP 133 Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data; Adopted on January 10th, 2007.
[7] WP 154 Working Document: Setting up a framework for the structure of Binding Corporate Rules
[8] WP 155 Working Document: Frequently Asked Questions (FAQs) related to Binding Corporate Rules

Mutual recognition of the lead DPA's approval

AmCham EU applauds the recent (October 1st) announcement of nine DPAs to agree on mutual recognition of BCRs - i.e. once a lead DPA has approved a company's BCRs the remaining DPAs should accept this approval and not "continue" the approval process by adding more comments. We call upon the remaining DPAs to follow suit as soon as possible in order for the scheme to be truly viable and to avoid having each DPA making their own comments and observations on the application which takes time and resources to deal with and results in inconsistency.

Nature of obligations

Many organisations, including existing applicants are now actively questioning the use of BCRs as a compliance strategy. Not only is the approval process time consuming and expensive, but the final solution is often more onerous than that of other alternatives, such as standard contractual clauses, as BCR require additional obligations relating to training, audit and co-operation with regulators. DPAs should bear this in mind when reviewing applications for BCRs and should not seek to interpret these requirements in an onerous fashion or impose additional obligations on applicants beyond those contained in Article 29's working document. AmCham calls on all DPAs to take a measured and proportionate response to BCR applications to ensure they remain a viable compliance strategy.

Standard Contractual Clauses

The adoption of the alternative set of Standard Contractual Clauses for data transfer between controllers, which was developed by AmCham EU together with other trade associations has been widely welcomed by our members who have increasingly relied upon them as a means to legitimise the transfer of data to third countries not offering an adequate level of protection.

However, a number of practical difficulties remain and some aspects in the functioning of these clauses could be improved or clarified:

Introduction of multi-party Standard Contractual Clauses

Although the Standard Contractual Clauses are drafted as bipartite contracts, both the Article 29 Working Party and the Commission have stated that they support the use of Standard Contractual Clauses in a multi-party context.

In its Working Document WP 74, the Article 29 Working Party commended the use of Standard Contractual Clauses involving multiple parties:

> "*…after the Commission decisions on standard contractual clauses and the considerable guidance provided by this Working Party and national data protection authorities, companies are making broad use of these instruments in a very positive and encouraging way (eg, the standard contractual clauses with many parties to the contract).*"

The Commission provided similar support for multi-party Standard Contractual Clauses in its Staff Working Document of January 20th 2006[9], which contains the following section:

> *"a) The use of master agreements*
>
> *[…] The Commission services see no objection to the subscription of standard contractual clauses by several data exporters and/or importers as long as it is made very clear that the information must be provided with the same level of clarity and specificity that is currently foreseen in Appendix 1 for a single data exporter and a single data importer."*

This general approval has also been adopted by some DPAs, such as the UK's Information Commissioner whose guidance on international transfers, issued in June 2006, states:

> *"if the only change to the model clauses is to make the contract between more than two parties (eg. where there is more than one data importer) rather than remain a bilateral agreement between one data exporter and importer then the Commissioner is of the view that this does remain within the scope of the Commissioner's authorisation provided that the obligations of all the parties remain clear and legally binding."*

AmCham EU welcomes the proposal for an extension of the use of Standard Contractual Clauses in a multi-party context. We call upon DPAs in other member states to heed the position of the UK Information Commissioner on this topic.

Uniform and streamlined procedural requirements when using Standard Contractual Clauses

It is our understanding that the original intent of the European Commission was that entities using and complying with, the Standard Contractual Clauses would not need to meet any other requirements in order to comply with the trans-border data flow obligations in the directive.

[9] Commission Staff Working Document (SEC (2006) 95) on the implementation of the Commission decisions on standard contractual clauses for the transfer of personal data to third countries (2001/497/EC and 2002/16/EC); Adopted on January 20, 2006.

However, the procedural requirements for Standard Contractual Clauses are not uniform throughout the member states. As a result, DPAs take varying approaches to the notification and/or approval of Standard Contractual Clauses, even when presented verbatim for approval as simple bilateral agreements.[10]

Moreover, the level of detail required in the schedules to the Standard Contractual Clauses varies greatly among member states. Some DPAs require only a general overview of the types of data transferred, whereas others require very detailed information about these data flows. The rationale for requiring detailed information in the schedules remains unclear. Considerable effort is required with little discernable benefit: the data inevitably becomes outdated within a short period of time.

In the short term, AmCham EU urges the Commission (via the Article 29 Working Party) to draw up a report on the data controllers' obligation to file a copy of the Standard Contractual Clauses to DPAs. This would be a very useful tool for data controllers.

In the long term, the Commission should try to ensure that DPAs have uniform procedural requirements. These should only oblige data controllers to deposit a copy of the Standard Contractual Clauses with a DPA and should prohibit DPAs from requiring overly-detailed information in the schedules unless there are exceptional reasons justifying this requirement.

These changes would remove some of the key bureaucratic and administrative barriers to the use of Standard Contractual Clauses and lead to much greater use amongst international organisations.

Onward transfers to processors

The ability to make onward transfers of data to a data processor has not been properly dealt with in the various sets of Standard Contractual Clauses, even though such onward transfers are common in practice.

Our members call upon the Commission to introduce adequate procedures to allow onward transfer to a data processor (possibly via the Working Party 29). In particular, it should be possible for the data importer to outsource the processing to other processors within a clear legal framework. A set of processor to processor clauses could also be envisaged.

Adding more clauses to the Standard Contractual Clauses

[10] We are aware that National Data Protection Authorities in at least France, Germany, Italy, Luxembourg, the Netherlands and Spain require the Standard Contractual Clauses to be notified to them, and in some cases a permit is required.

Answers to the Frequently Asked Questions (FAQs) accompanying each of the three sets of Standard Contractual Clauses issued to date by the Commission have all confirmed that additional clauses may be added. One particularly relevant answer states:

> *"Parties are free to agree to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses approved by the Commission or prejudice fundamental rights or freedoms of the data subjects. It is possible, for example, to include additional guarantees or procedural safeguards for individuals (eg, on-line procedures or relevant provisions contained in a privacy policy, etc)."*

AmCham EU considers that including additional clauses such as confidentiality clauses when using Standard Contractual Clauses is crucial for their business and welcomes the clarification provided in that respect by the Commission.

Specific Standard Contractual Clauses for HR transfers

Transfers of HR data should be facilitated. We suggest that a specific set of Standard Contractual Clauses be adopted to enable the sharing of employee data within a group of companies and with external providers of human resources services (such as payroll administration). This new set of clauses should be flexible enough to deal with the inevitable changes in the type of data actually transferred.

Consent – Article 26(1)

One of the available exceptions under Article 26 (1) often relied upon is the "unambiguous consent" by a data subject to a transfer.

The Article 29 Working Party published a report in 2005 entitled: "Working document on a common interpretation of Article 26 (1) of the directive"[11]. In this report, the various options for transferring personal data were explored. AmCham EU agrees with the Working Party that "the interpretation of Article 26 (1) must necessarily be strict".[12] However, that does not mean that consent should be more restrictively applied than other alternatives under the directive.

According to the report, the following requirements need to be met in order to use consent as a valid means to transfer personal data to third countries without adequate data protection:

[11] WP 114 Working document: Common interpretation of Article 26(1) of Directive 96/46/EC of 24 October 1995;" adopted on November 25th, 2005.
[12] See page 7 of the WP 114 Report.

- Consent must be a clear and unambiguous indication of wishes
- Consent must be given freely
- Consent must be specific
- Consent must be informed[13]

These requirements by themselves are not surprising. The directive itself already provides a definition of "consent":

> *"(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."*[14]

Article 26 (1) of the directive clearly states that in order to qualify as a derogation under which data may be transferred, the consent needs to be "unambiguous." This means that all requirements mentioned by the Working Party are directly based on the text of the directive itself. The only exception would be the requirement that consent must be a "clear" indication of wishes. However, that coupled with the requirement that the consent must be unambiguous does not seem to impose an extra requirement.

In various instances, companies may want to rely on consent and will do the necessary to make this a legally acceptable derogation. The fact that consent is often asked for in an on-line environment is not a roadblock. Boxes are commonly used to provide the data subject with a familiar and easy way to express his or her opt-in with a certain choice. Instead of using pre-ticked consent boxes, often companies go the opposite way and offer pre-ticked boxes for the "do not consent" option. This means the data subject needs to actively change the pre-ticked option in order to provide an unambiguous consent.

In the report, the Working Party noted that data subjects who are employees would not be able to provide a freely-given consent due to the existing relationship of subordination between employer and employee.[15] While asking for individual consent indeed will neither be a proper nor a practical legal basis for the transfer of large quantities of data on existing employees, it can still be a valid derogation for many other applications. The Working Party only points out that "there will be cases" where consent would work. However, that incorrectly suggests that using consent would only be allowed in a very limited number of cases.

The use of consent should be allowed in a range of cases, particularly when companies would like to transfer employee data for specific purposes. In practice, consent should still be accepted as a derogation for many data transfers, particularly the transfer of (some) employees' business contact data or other personal data of a less confidential character.

[13] See page 10 and further of the WP 114 Report.
[14] Directive article 2 (h).
[15] See page 11 of the WP 114 Report.

Consent should be acceptable for data transfers in the context of, for example, administration of stock option plans by a third party (eg, a bank) or by a country outside the EEA. Other examples include: the completion of on-line training courses, the inclusion of business contact data in a "people finder" system, the management of company cars, the collection of appraisals from co-workers in different countries or the posting of job vacancies with a tool to reply and file a Curriculum Vitae. All of these systems serve clear business purposes and are most often also in the interest of the employees or potential employees themselves. Even if a company has other viable alternatives, it would be illogical to rule against consent as a valid derogation, because the employee did not have a genuinely "free" choice.

Going one step further is the idea that persons applying for a job in a multinational company will have to accept the fact that for various HR management functions their personal data may have to be centrally processed and can be shared with data processors in third countries. They can make a deliberate choice whether or not they prefer to work for a multinational company which will mean they are asked to agree with data sharing, or whether they prefer to work for a company that is not part of a multinational and that will keep their personal data in the country where they will be employed. The details about the personal data that actually are processed can be provided in a separate document or by maintaining an intranet website that provides all information dealing with the protection of personal data. Of course this would not set aside the obligations of such a company to comply with the general principles for the collecting and processing of personal data. Also the purposes would have to be limited to HR management and could not, without explicit consent, include eg, selling products or services to the company's employees.

The requirements that the consent be "specific" and "informed" are uncontested. Consent would be specific for the purposes described above. Of course employees need to be adequately informed about which personal data is transferred and for what purpose. In various member states, Works Councils are involved in approving systems that process and transfer personal data. This provides a further guarantee that the information employees receive before being asked to provide consent will be adequate. Of course, employees may ask their HR department to provide further information on the transfers of personal data taking place. Ultimately, employees can also use their legal rights to access their personal data or, should there be sufficient reason, file a complaint with the national DPAs.

In summary, AmCham EU would highlight that consent should be an acceptable legal basis for transferring personal data to third countries, in particular relating to employee data for specific applications, provided adequate prior information is provided. For new employees including a consent clause in the employment agreement on the international sharing of their employee data for HR management purposes must be allowed as well.

Commission Adequacy Decisions

Adequacy for international data transfers can be ensured in a number of ways, as we have outlined in this paper. One other way is via Commission adequacy decisions where the Commission accepts the adequacy of data protection systems in non-EEA countries.

As noted above, bilateral agreements have been reached with Argentina, Canada, Guernsey, the Isle of Man, and Switzerland. AmCham EU would encourage the Commission to increase the number of bilateral agreements with non-EEA countries to facilitate international data flows, such as: Australia, Dubai, Japan, Korea and New Zealand, all of which have data protection laws in place.

During the last few years, agreements with the United States have focused on the specific issue of transfer of Passenger Name Record (PNR) data by air carriers to the US Department of Homeland Security. Discussions have proven difficult as they deal with the core issue of how to strike a balance between law enforcement and data protection requirements. AmCham EU supports the ongoing dialogue between EU and US authorities in this matter.

Safe Harbour Agreement

The other main bilateral agreement reached between the EU and the US resulted in the Commission's Safe Harbour Decision of July 2000, which established a mechanism for transferring data between the EU and those US companies which adhere to the seven Safe Harbour principles[16].

AmCham EU is very supportive of the Safe Harbour Agreement and encourages its continued use. However, the Agreement does not currently cover transfer of data by companies with financial services (other than HR personal data) or telecommunications operations – as both of these sectors fall outside the scope of the Federal Trade Commission's (FTC) jurisdiction. AmCham EU vehemently supports extending the coverage of the Safe Harbour Agreement to these currently excluded industry sectors.

In 2002, the Commission published its first report on the functioning of Safe Harbour, followed up by a more in-depth report in 2004.[17] The reports showed that the system, in general, works well. However, the Commission pointed to certain areas which could be improved, eg, that some companies had published a privacy policy that was

[16] The seven Safe Harbor Principles are: Notice, Choice, Onward Transfer, Security, Data Integrity, Access, and Enforcement.

[17] Commission Staff Working Document (SEC (2004) 1323) on "The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbor Privacy Principles and related Frequently Asked Questions issued by the U.S. Department of Commerce," Adopted on October 20th, 2004.

not compliant with the Safe Harbour principles or that the US Department of Commerce as the competent body for ensuring self-certification should improve its website to enhance transparency. However, many of these shortcomings have been successfully addressed since the publication of the report in 2004.

AmCham EU members who have signed up to the Safe Harbour Agreement believe the process for adhering to its principles and the yearly renewal of the self-certification process are not overly burdensome. It is a well-structured process and provides a useful exercise for the companies involved. In addition, companies benefit from very helpful cooperation from the US Department of Commerce in completing the process. Moreover, the success of the Safe Harbour programme is proven by the constant growth of its membership (more than 1,500 signatories). AmCham EU is keen to see that this mechanism continues to allow for the free flow of data to Safe Harbour companies.

One way of using Safe Harbor that does not seem to be used in a lot of cases is the option for data processors established in the US to certify for Safe Harbor not in relation to their own personal data (eg, of their employees working for their European subsidiaries) but for the personal data they would be processing for their European clients. In FAQ 10 of the Safe Harbor decision it is clearly indicated that this is a possibility[18]:

> "Because adequate protection is provided by safe harbor participants, contracts with safe harbor participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the member states) as would be required for contracts with recipients not participating in the safe harbor or otherwise not providing adequate protection."

As is the case with Standard Contractual Clauses, where data processors have self-certified compliance with the Safe Harbor principles, the existing rules are not very clear on how to provide a legal solution in case the data processor wants to use subcontractors that have not joined the Safe Harbor program, or are located in third countries. When a US data processor operating globally joins the Safe Harbor program in relation to the personal data of its clients and would like to involve various of its subsidiaries globally in the processing of such data, such company should also be allowed to make the certification on behalf of all those subsidiaries. That would mean that the enforcement measures that are part of the Safe Harbor program would also be directed towards the US data processor in relation to possible infringements made by one or more of its foreign subsidiaries.

18 http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l_215/l_21520000825en00070047.pdf

Conclusion

AmCham EU underlines the necessity of workable solutions for businesses regarding international transfers of personal data in a globalised world economy. In our view, it is essential to reduce the massive requirements for business imposed by differing implementation of the directive in the 27 EU Member States. Therefore, we welcome any efforts to build upon the already existing exceptions under the directive to further improve the management of personal data in an international context.

AmCham EU is deeply committed to a close dialogue with relevant authorities to advance these issues and is looking forward to ongoing collaboration.

* * *

The American Chamber of Commerce to the European Union (AmCham EU) is the voice of companies of American parentage committed to Europe towards the institutions and governments of the European Union. It aims to ensure a growth-oriented 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. Total US investment in Europe amounts to €702 billion, and currently supports over 4.1 million jobs.

* * *