EUROPE
TechAmerica

THE ASSOCIATION OF COMPANIES DRIVING INNOVATION WORLDWIDE

TechAmerica Europe comments for Informal JHA Minister meeting on Transfer of Personal Data to Third Countries

Brussels, 20 January 2014

TechAmerica Europe represents leading European high-tech operations with US parentage. Collectively we invest Euro 100 bn in Europe and employ approximately 500,000 Europeans. TechAmerica Europe Member companies are active throughout the technology spectrum, from software, semiconductors and computers to Internet technology, advanced electronics and telecommunications systems and services. Our parent company, TechAmerica is the leading tech association in the US.

This paper has been put together in preparation to the upcoming Informal JHA Minister Meeting on 23-24 January and builds on both, the work of the DAPIX working group to date (16 December: 17831/13), and the report adopted by the European Parliament's Civil Liberties (LIBE) Committee.

Introduction

TechAmerica Europe (TAE) welcomes the ongoing efforts of the Council to find the right balance between facilitating the free flow of information and safeguarding the personal data of European citizens in a global context. Users as well as business are participating in a physical and online world which crosses jurisdictions' borders and hence requires a framework that includes instruments that allow for the international transfers of data which are in accordance with appropriate safeguards.

Being able to move data quickly, securely and legally around the world is a key factor in bringing the benefits of the internet to citizens. The proposed data protection regulation will build on a body of law that allows this to happen in a secure legal framework where companies, individuals and Governments understand their rights and obligations.

It is estimated that by 2016 about 1.3 zettabytes (the storage capacity of about 328 billion DVD's) of online data will flow across borders annually. Transborder data flows have become the backbone of international commerce and services. The internet economy alone has accounted for 21% of European economic growth during the past five years. Further, it is estimated that by 2015, the internet economy will be contributing 4-7% of GDP across most European markets.

Given the importance of international data flows we need a toolbox of legal measures we can use to move personal data cross border. This toolbox should include, amongst other mechanisms:

1. Binding corporate rules
2. Model contract clauses
3. Adequacy decisions both territorial and sectorial (such as the safe harbor)
4. Other suitable safeguards based on accountability of those who process data (including codes of conduct and other tools).

These instruments can be used depending on the type and nature of the data transfer; nevertheless the Regulation is an opportunity to extend the options available to legitimately transfer personal data. We urge the Council and Parliament not to shut down a company's ability to move personal data cross border. It is vital to the growth of the digital economy in Europe, a fact confirmed by the increasing number of SMEs exploiting the benefits of online services to create jobs in Europe. Data is critical to the ability of SME's to compete fairly in the global economy as was rightly highlighted by the European Commission Communication on "Rebuilding Trust in EU-US Data Flows". Here the Commission states that cross border data flows "form an integral part of commercial exchanges across the Atlantic including for new growing digital businesses, such as social media or cloud computing, with large amounts of data going from the EU to the US."

In the wake of the NSA revelations, we have seen a dangerous trend toward conflating commercial collection with unwarranted government surveillance. Data collection and "secret, unauthorized data collection" are two different things. Attempting to punish companies—both located in the EU and elsewhere—for unwarranted government actions only shifts blame to companies who have been caught in the middle. Constraining business will merely result in lost opportunities for EU citizens while governments are free to innovate in the area of surveillance.
The transfer of personal data to third countries is therefore a crucial element of the Regulation. A well-functioning regime on international data transfers is needed if the regulation is to achieve its goal to be a legal framework that is fit for the 21st century. We therefore welcome the opportunity to comment further on Chapter V.

Confirm that EU rules should apply to data controllers established in third countries when personal data of EU residents are being processed in the following context, namely: a) offering of goods or services, irrespective of whether a payment by the data subject is requested, to such data subjects in the EU; or b) the monitoring of data subjects' behaviour as far as their behaviour takes place within the EU.

The Regulation should contain clear rules defining its material and geographic scope of application, including provisions that deal with conflicts of law and extraterritoriality. The current proposals on geographic scope require further thought and Member states should consider proposing criteria to easily define cases where a global organization that handles EU individuals' data fully falls under the scope of the Regulation.

With this context in mind, we suggest that Member states consider the criteria defined in ECJ case law to determine the applicability of EU law. Neither the Commission proposal nor the current Council text take into account ECJ jurisprudence with regards to the extraterritorial application of EU law (rf. Altenhof case), requiring a targeting or directing criteria. For example the mere availability of goods and services to an EU audience should not, in itself, trigger the application of EU law. Therefore, we believe that the proposal requires further thinking to ensure clarity for business when they fall under the scope of the regulation.

It is not justified in the text why the use of a particular technique enabled by various technologies, i.e. profiling (rf. Recital 21), should be used as a criterion to define the extraterritorial scope of this Regulation. Such a provision would clearly go against the principle of technology neutrality included in Recital 13. It is important to provide legal certainty to non-EU based operators that can be accessed by individuals residing in the EU and not to undermine the stability and legal predictability of what should remain a principle-based framework.

The limitation in Article 3(b) to "as far as their behaviour takes place within the European Union" has improved the text. Otherwise, the proposal would have extended the scope of the regulation to controllers established outside the EU when their profiling activities would have included the activities outside the European Union. This would have required organisations to identify the data subject, contrary to the concept of data

minimisation. We believe that provisions on international transfers in Chapter V should be applicable in cases where personal data is not processed in the EU and transferred outside the EU.

Indicate how the protection of rights and freedoms of individuals should be ensured when the transfer of personal data to third countries is based on derogations from an adequate level of protection (adequacy findings or appropriate safeguards).

Unfortunately, the recent revelations on government surveillance practices have caused a dangerous trend towards mixing up the legitimate, commercial use of data with the unwarranted collection of data by various governments. While it is completely understandable that different procedures and tools are scrutinised, we believe that the criticism towards certain processes which aim at the transfers of personal data by corporate entities has been rather ill-informed and not proportionate.

It should be noted that adequacy findings are not derogations from an adequate level of protection; on the contrary, adequacy findings are the main tools that both the current Directive and the proposed Regulation put at the disposal of organizations to legitimately transfer personal data outside the EU. An adequacy finding is confirmed in a binding Decision of the European Commission and states the terms under which a country affords an equivalent, or adequate, level of protection. However, the European Commission's power to explicitly prohibit data transfers to a third country, territory or sector creates a risk for industry and does not provide citizens with any additional safeguards.

Affording an adequate level of protection over EU individuals' data is also not at odds with facilitating international data flows. Restricting data flows is not the best way to ensure an adequate level of data protection; the emphasis should instead be placed on the protection and subsequent use, not on restricting the transfer of data outside the EU.

The Commission proposal, building on the provisions of the 95 Directive (Art. 25) allows for adequacy rulings to apply to certain processing sectors or territories within a third country as well as to a third country as a whole. The explicit inclusion of sectorial adequacy rulings by the Commission improves the text. However, the European Commission's power to explicitly prohibit data transfers to a third country, territory or sector creates risk for industry and does not provide citizens with any additional safeguards.

As discussed during the Friends of Presidency meeting in September, the introduction of specific sunset/ review clauses (as later adopted by the European Parliament's Civil Liberties LIBE Committee) would create enormous legal uncertainty and would harm relations with trade partners and users unnecessarily. Similarly, the so-called article 42 (or article 43(a) at the European Parliament's LIBE Committee report) seems to be a misplaced idea to increase data subject's protection. Instead of taking addressing the core of the issue - unchecked governmental surveillance- companies are victimised for unwarranted government actions. This approach only distracts from the real issue and puts companies in a situation where they are caught in the middle of conflicting legislation.

We fully agree that greater transparency is needed around law enforcement requests for access to data and more needs to be done with regards to this challenge. However, we believe that the data protection regulation is not the appropriate forum for addressing these complex issues relating to governmental access to data and mutual legal assistance.

With regard to transfer of personal data to third countries, indicate whether the models referred in the draft Regulation (adequacy findings/appropriate safeguards, binding corporate rules, derogations as mentioned in Art. 44) are sufficient or alternative models and /or variations of the proposed models should be considered.

Generally, we believe that the chapter on international data transfers in the current proposal improves the situation for business by including considerably more detail on how to ensure compliant data transfers as well as by harmonising the rules. The statutory introduction of Binding Corporate Rules (BCR's) in Article 43 is extremely welcome. Further, we welcome the Council's intention to extend the scope to "groups of undertakings engaged in a joint economic activity". However we would encourage Member states to extend BCR coverage to processors and its sub-processors. This would better suit the needs of current data flows, especially in the context of the delivery of Internet-based computing services—"cloud computer"—and assure that no matter how many subcontractors are engaged in data processing, an adequate level of protection is afforded.

We believe that there is an opportunity for the Council to take better account of the concept of "accountability". Article 44(1), for example, seems to permit data transfers based on compliance with accountability requirements but unfortunately, it restricts organisations ability to show adequate safeguards for data transfers to sporadic and infrequent transfers. There is no justification for this limitation since neither amount nor frequency of the transferred data is relevant as long as appropriate safeguards for the protection of data subjects are in place. We would therefore recommend replacing the current reference to sporadic and infrequent data transfers by linking it to safeguards instead. Apart from Article 44(1), we want to clarify the potential role that certification schemes and code of conducts could play as additional accountability-based tools.

As mentioned before it is important to avoid sunset clauses or expiry dates attached to adequacy decisions as they create unnecessary legal uncertainty and risk lowering the levels of effective data protection. Including in the Regulation a clear rationale for a review with objective criteria for evaluation could help determine when a review is required.

Finally, attempting to address issues such as law enforcement and government agency access to data within the international transfers chapter of the regulation creates a compendium of conflict of law rules. These issues should be elsewhere, through existing mechanisms such as treaty agreements between governments.

Safe Harbour

We believe that the EU-US Safe Harbour framework provides significant economic benefits to Europe's economy. Many US organisations that self-certify to Safe Harbour do so following the request of their European partners while at the same time, many US subsidiaries of European organisations are using Safe Harbour to transfer data as well. In total, more than 4000 organisations have signed up to the principles laid out in the Safe Harbour decision. More than 50% of the participating organisations are SME's from both sides of the Atlantic. Techamerica Europe's members have found this a very useful tool that provides legal certainty for both, data subjects and the participating organisations.

Compliance with the framework requires that each organization that has self-certified its adherence to the framework reaffirms its commitment each year no later than the anniversary of the date on which its original self-certification was finalized. The self-certification requires a thorough internal review process and involves considerable organisational investments. TechAmerica Europe's members that have certified are aware of their responsibilities and have internal or external compliance programs in place.

The Safe Harbour framework has often been criticised for the lack of enforcement. Our experience, however, has demonstrated that these claims are not substantiated. The US Federal Trade Commission (FTC) has brought several enforcement actions which resulted in consent decrees that ensure the protection of European citizens.

We think that the Safe Harbour framework provides a valuable and strict tool for European and US organisations to transfers data across the Atlantic, as well as protecting Europeans' data sufficiently. Moving forward, improvements could be made to increase the value of Safe Harbour. We recommend that data processors established in the US can certify for Safe Harbor as well. They would have to apply the principle of data security themselves and for the other principles required for compliance, they need the cooperation of their European data controller (customer). For data processors who receive personal data from their clients located in the EU such certification could be very useful.

Managing the scope of government surveillance and using data for commercial purposes are two different issues. Safe Harbour is designed for commercial data flows and is essential for businesses and citizens on both sides of the Atlantic. We don't believe that the Safe Harbour framework needs a major makeover, but a review that is tied to achieve tangible improvements in its implementation could be meaningful. Nevertheless, it cannot be conducted at the expense of legal certainty for companies and data subjects and should not lead *a priori* to the suspension of the existing agreement or the setting of a sunset clause.

For further information please contact:

[redacted]
Rue de Namur 16
1000 Brussels
[redacted]