BUSINESSEUROPE

STATEMENT

31 March 2015

BUSINESSEUROPE input in view of the revision of Safe Harbor

SAFE HARBOR NEEDS TO BE REINFORCED, BUT IT MUST REMAIN IN PLACE

In the context of the current review of Safe Harbor, BUSINESSEUROPE urges the Commission to maintain the framework in place and strengthen its security at the same time. Safe Harbor is a key instrument to transfer personal data from the EU to the US. Some of its elements, such as enforcement and scope, must be revised. Encryption and other technical solutions could be encouraged to make Safe Harbor safer, but must not be made mandatory. Transparency must be ensured and companies should be able to disclose to what extent they share data with public authorities for purposes of national security. The recent developments about government surveillance have damaged citizens' trust and had serious negative implications for companies and for the digital economy as a whole. Governments must ensure a proper balance between national security and respect of citizens' fundamental rights. However, the debate on the scope and implications of mass surveillance activities from national governments needs a much broader political solution that goes beyond Safe Harbor.

Introduction

The ability to transfer data is crucial for companies everywhere in the world, no matter their size or the geographic area where they operate. Data flows are an integral part of today's international trade. As practical examples, data flows are needed for more accurate health diagnoses, improved logistics and smarter energy use. Companies and consumers collect, analyse and transfer data in order to take advantage of the digital economy and exploit the potential of the Internet. Transferring data is also part of the internal functioning of companies.

In this context, Safe Harbor is a convenient and efficient tool for companies to transfer personal data to the United States. Recent developments have questioned whether this instrument is providing adequate protection for EU citizens. The Commission has addressed a number of recommendations to the US authorities in order to improve this framework.

Trust of consumers and businesses in the digital economy is fundamental to take advantage of the new opportunities ahead. Innovations such as cloud services, data analytics improving efficiency in industrial processes and intelligent connected machines could add more than €2000 billion to Europe's GDP by 2030. BUSINESSEUROPE supports the efforts towards the improvement of Safe Harbor. We believe Safe Harbor should be strengthened, but a potential suspension of this framework is not an option - because of the negative consequences this would imply - and we urge the Commission to carefully take them into account.

AV. DE CORTENBERGH 168
BE-1000 BRUSSELS
BELGIUM
VAT BE 863 418 279

BUSINESSEUROPE a.i.s.b.l.
WWW.BUSINESSEUROPE.EU

TEL +32(0)2 237 65 11
FAX +32(0)2 231 14 45
E-MAIL: MAIN@BUSINESSEUROPE.EU
EU Transparency register 3978240953-79

I. Safe Harbor is a key instrument for EU companies to transfer data to the US

Safe Harbor allows the transfer of personal data from EU Member States to companies in the US which have signed up to the principles of this framework. It aims at securing an adequate European standard of data protection for EU citizens when data is transferred to the United States. The system does not require mandatory notification or request for authorisation from the Data Protection Authorities (DPA), avoiding administrative burdens and additional costs for both DPAs and companies. SMEs account for 60% of Safe Harbor participants. They can benefit from the streamlined and cost-effective compliance requirements, often preferred to Binding Corporate Rules (BCRs) or standard contractual clauses, more complicated and costly. SMEs would therefore be most likely the ones suffering most from suspending Safe Harbor.

Businesses use Safe Harbor not only to process customers' data, but also to transfer other personal data (for instance, employees' data). These processes are done on a permanent basis, and they are part of the internal functioning of certain companies.

BUSINESSEUROPE supports an improvement of the system. The transatlantic cooperation to ensure reliable data protection must be strengthened. Safe Harbor needs to be updated to respond to the current and future challenges. If the European level of data protection is not enforced to US companies that process EU citizens' data, there is a risk of creating an uneven level playing field. However, the suspension of this mechanism is not the right solution to address the existing challenges, as it would disrupt the current data transfer mechanisms, creating legal uncertainty, additional costs for businesses and administrative burdens. For instance, US commercial partners that are self-certified under Safe Harbor and are providing services to European companies would have to find alternative systems of transfers, such as standard contractual clauses or BCRs. This adaptation would be burdensome. It must be also taken into account that BCRs for controllers only work for groups' internal transfers, and that in some Member States they are not codified. BCRs therefore would not be an alternative mechanism for data transfers in most cases, requiring companies to go for national ad-hoc authorisations by DPAs. Moreover, the suspension of Safe Harbor will not address the EU institutions' concerns, as data would still be transferred to the US trough the alternative transfers mechanisms mentioned above, using different tools but raising identical concerns.

That said, currently there are significant **implementation and enforcement** deficits in Safe Harbor that need to be addressed. Companies should do more than merely claiming compliance with European standards. The Federal Trade Commission (FTC), responsible for the enforcement of Safe Harbor, should step up its control mechanisms and is making positive steps in this direction. It is important that this framework comprises a minimum set of controls before a company adheres to Safe Harbor, namely a system of regular checks on certified companies, with effective sanctions for violations including economic penalties. Effective monitoring by US authorities is also essential, for instance through annual reports on how Safe Harbor principles are being implemented and external audits on randomly chosen Safe Harbor adherent companies.

The **scope** of Safe Harbor must be broadened too, and cover the whole chain of data processing. The current Safe Harbor framework excludes certain sectors, such as the telecommunication, financial and insurance sectors. When the Safe Harbor principles were agreed in 2000, digital business models were different compared to how they are today. Now, in certain cases, companies in different sectors provide the same services (which may require the transfer of personal data from the EU to the US), thus competing with each other. In this context, the possibility to use Safe Harbor to transfer data must be given to all actors in the value chain providing the same kind of services. Given the evolution of digital business models, the scope of application of Safe Harbor should be based on the type of service rather than on the sectors.

II. Encryption and other technical solutions can be useful to improve safety, but are not a panacea

BUSINESSEUROPE believes that **encryption and other technical solutions could be encouraged but should not be made mandatory**, being mindful of the operational costs and effort involved. Mandating the use or a certain approach to encryption or other technical solutions would not be the right approach, as it would stifle innovation and increase inefficiencies and cost for businesses without demonstrable benefits.

The possibility to encrypt data has entered the debate as a possible means to strengthen the safety of international data transfers and solve the issue of trust. Encryption technologies are widely available and already used as standard practice by large and small businesses to improve security of data. There are a wide variety of tools, from low cost instruments offering basic security, to highly sophisticated techniques with high levels of encryption. It must be taken into account that the higher the level of encryption used, the less wieldy the data become.

Technical solutions are not the answer to avoid mass surveillance. In order to prevent such episodes, political consensus and legal requirements (not technical ones) are essential.

It should also be noticed that companies are obliged, in the EU and in the US, to deal with requests for access to data through existing procedures such as Mutual Legal Assistance Treaties (MLATs). MLATs are a key tool for addressing extraterritorial law enforcement access to commercial data. They can reduce unnecessary and disproportionate burdens on companies by enhancing the effectiveness of cross-border lawful access to personal data by enforcement agencies. In this context, the issue of encryption – as well as of encryption keys' management - should be carefully evaluated, in particular with regards to who owns the keys and how judiciary authorities could have access to them.

Another challenge related to encryption is that it could limit the ability of telecom operators to manage the security of the networks. In some cases, encryption could limit operators' ability to perform the data traffic monitoring tasks entrusted to them for public security and law enforcement purposes, for instance to comply with lawful interception requirements.

Furthermore, mandatory end-to-end encryption may not be an appropriate means to ensure adequate protection of personal data in certain data processing scenarios, e.g. in cases where a service provider, in its capacity as Safe Harbor certified data processor, remotely accesses IT systems of a European based controller for trouble shooting purposes only.

Finally, a possible obligation on Safe Harbor companies to encrypt data would not affect the transfer of data allowed under other mechanisms such as standard contractual clauses or Binding Corporate Rules, undermining the level playing field and leaving the challenge posed by rules governing access to company data unsolved.

III. Transparency must be ensured when transferred data are accessed by national authorities

Transparency is a must. Users need to be able to trust the digital world and the mechanisms to transfer data, within Europe and outside. In this context, trust and security are amongst the most difficult challenges for data-driven innovation.

Companies should be put in a position which enables them to disclose to what extent they share data with public authorities for purposes of national security. EU citizens and EU companies should be able to access US Courts for claims related to breaches of data protection rules.

IV. The issue of surveillance needs a broader political solution

Surveillance is not only a Safe Harbor related matter. The ongoing Safe Harbor review should be considered as one specific element of a broader political debate on the scope and implications of mass surveillance activities from national governments. This topic still needs a political solution.

The recent developments concerning governmental surveillance programmes have seriously damaged citizens' trust in cross-border data transfers and generally in the online world. The revelations about governmental surveillance programmes had an extremely negative impact on companies which rely on collection and use of data. The digital economy was seriously damaged. For example, according to surveys, individuals are less likely to use certain cloud services in light of the recent revelations.

Governments must ensure a proper balance between national security and respect of citizens' fundamental rights. They should avoid any actions that might undermine Internet security, for example by inserting vulnerabilities. These actions undermine citizens' trust, creating prejudice to companies which use personal data and damaging the whole global digital economy. Exemptions on data protection principles for national security purposes should be proportionate and reduced to a minimum.

Surveillance activities must contain measures for effective, independent and impartial oversight, as well as remedial measures. Adequate safeguards must be ensured regarding the purpose of use of such data, the time of processing and the further actions on the data when they become obsolete for the purpose for which they were disclosed. Compliance with law enforcement requests should neither require companies to violate data protection or privacy laws of other countries, nor their reasonable commitments to individuals, employees, and customers.

One way to move the discussion forward would be to call for a government-to-government discussion on how surveillance should be conducted, ensuring the use of the least harmful technological measures available. The prescriptions contained in the current EU data protection framework should be preserved: "Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected". A multilateral forum for discussions, involving a range of stakeholders, from governments to businesses, could also be created to support this exercise.

Digital is crucial to ensure Europe's competitiveness and deliver growth and jobs. If they want to succeed in the digital economy, companies need to transfer data from Europe to other countries, including the US, and vice-versa, without excessively burdensome procedures or costs. Safe Harbor is an important instrument in this perspective and needs to remain in place. But companies also need security and trust of citizens to be able to operate in the digital single market. In this context, Safe Harbor needs to be substantially improved. BUSINESSEUROPE encourages the European Commission and its US counterparts to strike the right balance between these concerns. The revision of Safe Harbor must increase awareness on the importance of data protection as a fundamental right, without jeopardizing the necessary exchange between two of the most important economic areas on the globe.

* * *