BUSINESSEUROPE

POSITION PAPER

26 September 2014

The importance of cross-border data transfers for business

BACKGROUND

Data driven innovation is key for jobs and growth in Europe. It can leverage €330 billion a year in the EU by 2020. Data flowing across borders, combined with solid trust of users in the protection of their personal data, is a precondition for international trade, the digital economy and the internal functioning of European companies, large and small, operating internationally.

Data flows are important for consumers and businesses alike, impacting their everyday life. 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. Data flows are also crucial for public interest organisations, when, for example, they enable supply of emergency aid, nutrition and information during disaster relief. Companies and consumers collect, analyse and transfer data in order to take advantage of the digital economy and exploit the potential of the Internet.

Cross-border data transfer is a part of ongoing initiatives such as the proposal for an EU data protection regulation, as well as free trade agreements between EU and third countries. Revelations concerning governmental surveillance have weakened consumers' and companies' trust in the digital world and have placed the topic high on the political agenda, making it one of the main challenges for the digital economy.

Because of growing mistrust in data use and transfers, some countries have been discussing the possibility to force "data localisation", which means requiring local storage of personal data in one territory. There have been proposals from some Member States in favour of a European routing system, in which data would be routed within Europe's territory as much as possible. In the US, localisation of communication infrastructure, local routing and local data storage requirements are implemented on a case-by-case basis for specified types of data. This is done through bilateral network security agreements between US agencies and relevant operators as part of the review process to authorise foreign investments into critical infrastructure sectors. In addition, the European Parliament has recently called for the suspension of the Safe Harbor mechanism, which allows companies from specific sectors to transfer personal data from the EU to the US.

BUSINESSEUROPE a.i.s.b.l
AVENUE DE CORTENBERGH 168 – BE 1000 BRUSSELS – BELGIUM
TEL +32 (0)2 237 65 11 – FAX +32 (0)2 231 14 45 – E-MAIL MAIN@BUSINESSEUROPE.EU
WWW.BUSINESSEUROPE.EU
EU Transparency register 3978240953-79

CROSS-BORDER DATA FLOWS ARE ESSENTIAL FOR EUROPEAN BUSINESS AND INVESTMENT

International trade cannot take place without data flows

Cross-border data flows are relevant for companies in every sector, not only for IT companies or cloud providers, and of all sizes. Limiting the possibility of data flowing across borders without objective reasons would therefore be detrimental to competitiveness and growth of European companies.

International trade implies flow of data across borders. The OECD, WTO and UN concluded that success in international markets depends as much on the capacity to import high-quality inputs as on the capacity to export[1]. In many instances cross border data flows form an important element of high-quality inputs.

For consumers, the potential for e-commerce is still underexploited and therefore restricting the flow of data would limit even more their choice of goods and services. Companies need to be able to efficiently transfer data across borders in order deliver goods and services to consumers, process payments or provide customer support. On the other hand, it is important that such transfer is carried out providing adequate guarantees for the protection of personal data; otherwise, users will not be encouraged to use the new services, to the detriment of all parties. Trust and confidence are likely to be amongst the major challenges for the Internet and the digital economy. Ensuring digital confidence will allow businesses and consumers to fully exploit the potential of e-commerce.

Companies' daily operations need cross border data flows

International companies need to move data quickly in order to manage their global investments and efficiently control and run internal processes. They need to exchange data with headquarters, through affiliates, through regional centres, and through third party vendors. Companies need to transfer human resources data to and from headquarters. They also need to move data to and from R&D facilities that they set up abroad, often due to specific skills available in that country. Moreover, companies need to transfer data because of processes they have outsourced or cloud solutions they purchase to improve efficiency. Disruption of data flows can therefore be extremely problematic for complex value networks.

BUSINESSEUROPE RECOMMENDATIONS ON CROSS-BORDER DATA TRANSFERS

In this context, BUSINESSEUROPE has the following recommendations to ensure that the flow of data across borders can take place, while ensuring safeguards to protect citizens' personal data and enhance their trust in digital services:

[1] *Implications of Global Value Chains for Trade, Investment, Development and Jobs*, report presented to the G20 Summit, September 2013, http://www.oecd.org/trade/G20-Global-Value-Chains-2013.pdf

- ***Avoid the imposition of forced data localisation requirements.*** Local server and data storage requirements could lead to higher costs and reduced competitiveness for businesses. In addition, localisation of servers might also become a barrier, for example in cases where data need to be moved abroad for troubleshooting or other technical operations even if servers are local. Limiting data flows could also mean reducing the competitive advantage that international services can deliver to business and consumers in Europe and across the globe. Moreover, any data flow restrictions or local data storage requirements implemented in Europe could lead to similar restrictions in other countries, limiting the trade and investment opportunities of European companies.

- ***Encourage mechanisms to reinforce trust and security.*** Companies have a role to play in designing products for security and investing in security of operations. The development of technological solutions such as encryption of data, securing the integrity of data, avoiding security breaches and offering consumers a choice of privacy enhancing technologies are opportunities for companies to preserve customers' trust. They can also be a source of competitive advantage. The use of forms of data not attributable to a specific person (pseudonymous) could be encouraged by considering these data to be more secure than regular personal data and adapt rules accordingly. Furthermore, a debate on European routing, meaning that Internet packets sent from a European sender to a European receiver stay within Europe's borders as much as possible, is currently taking place. It is important to ensure a level playing field for EU and US companies at global level. We invite for open discussion on advantages and disadvantages of European routing before drawing conclusions. In this context, a careful assessment is needed on the impact of the recent European Court of Justice ruling on the EU Data Retention Directive. The Court notes that "the control (…) by an independent authority of compliance" with the requirements of EU law is "an essential component of the protection of individuals", and since the directive does not require data to be retained within the EU, it "cannot be held" that the aforementioned control of compliance is fully ensured. (ECJ Case C-293/12 and C-594/12, point 68).

- ***"Adequacy" requirements must be implemented properly in order not to unduly restrict international data flows.*** As a principle, cross-border data flows, processing and storage must be in compliance with data protection and security rules in force in the country of residence of the data subjects. In this context, policy makers should:

  - Promote and expand international harmonisation, such as mutual recognition or adequacy assessments of countries' privacy regulation, without requiring a competent authority to approve cross-border data flows, or controllers or processors to rely on specific legal transfer mechanisms, such as the Safe Harbor framework, EU binding corporate rules or EU standard contractual clauses.

  - Work for a continuous expansion of the application of data protection principles in additional countries to be approved as adequate. According to the draft data protection regulation, data transfers from the EU to a third country may take place if the country in question ensures an "adequate" level of protection. The assessment upon such adequacy must be performed timely, transparently and following clear, explicit and relevant criteria.

- Avoid excessively rigid safeguards. We understand the need for safeguards in case of transfers to a country upon which an "adequacy" decision has not yet been taken by the Commission. However, the safeguards must not be excessively rigid for companies or imply excessively long delays, in order to avoid disrupting business models. For instance, the requirement to obtain authorisation from the supervisory authority where transfers take place on the data controller's own standard contract clauses will create burdens for companies and delay processes significantly. In general, when legal transfer mechanisms such as the Safe Harbor framework, EU binding corporate rules or EU standard contractual clauses exist to handle different levels of stringency in different data protection systems, then additional approvals by a national competent authority should not be required for data transfers already covered by such mechanisms.

- ***Provide adequate rules for data transfers within groups of companies.*** The EP already followed a risk-based approach and recognised that the transfer of personal data within a group of undertakings of controllers in the EU does not impose a higher risk than transferring it within one legal entity. This principle should be expanded to processor groups of companies and should be introduced for third country transfers, if an adequate level of data protection in the third country is secured. The possibility for binding corporate rules to secure an adequate level of data protection in a processor-to-processor relationship should be introduced, allowing European processing entities to transfer data to their group companies abroad.

- ***Ensure the effective functioning of the Safe Harbor mechanism.*** Safe Harbor is a flexible instrument that allows European companies to transfer personal data to the US while at the same time ensuring that EU citizens' data is protected according to EU principles. BUSINESSEUROPE supports and encourages the efforts of the US authorities, responsible for the administration and the enforcement of Safe Harbor, to take into account the European Commission recommendations presented last November aimed at improving the system. These efforts will be necessary to avoid Safe Harbor's abrupt suspension, which would hamper global businesses and both the European and US economies. Moreover, BUSINESSEUROPE supports the revision of the framework to adapt it to the current challenges. In this context, we welcome the European Commission recommendations to improve Safe Harbor and we call for a timely conclusion of the current review process. For now, the revision should maintain the overall structure and principles in place, while reinforcing some elements, such as enforcement and transparency, subcontracting chain responsibilities and confidentiality clause exemptions. The participation in Safe Harbor should cover the whole chain of data processing. In addition, closer cooperation between US and EU authorities must be ensured and the scope of the framework widened to other sectors that are currently excluded.

- ***Take a coordinated approach to policy decisions.*** The functioning of cross border data flows has both an internal and an external dimension in the EU, with different policy implications. We call for stronger coordination between different services in the Commission and relevant Committees in the Parliament, as well as the involvement of all other relevant stakeholders. Before making any decision on legislative action with a significant impact on data transfers, the impact on the digital economy, industrial policy, consumers, international trade and the functioning of the single market should be taken into account. Member States

should be consistent and harmonised in their approach and decisions having implications on data flows.

- ***Avoid weakening trust in the digital environment.*** The recent developments concerning governmental surveillance programmes have seriously damaged citizens' trust in cross-border data transfers and generally in the online world. This has a negative effect on the digital economy. For example, according to surveys, individuals are less likely to use certain cloud services in light of the recent revelations on governmental surveillance programmes. Keeping the Internet strong means keeping it safe and maintaining trust. 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. Moreover, the willingness of people to share data is a fundamental prerequisite for a data driven economy, thus establishing and sustaining customer's confidence is critical. It is important that individuals feel they are in control of the information they share.

CONCLUSION

Trust and confidence are amongst the major challenges for a sustained growth of the digital economy. Ensuring that sensitive business and consumer data do not fall into the wrong hands and are not exploited for unlawful or unfair purposes is of vital importance for public administrations, businesses and consumers alike. BUSINESSEUROPE believes that adequate and properly enforced mechanisms for the protection and transfer of data are necessary to build trust in the online world and enable our societies to benefit from the vast potential of big data.

Protectionism and restrictions on the commercial use of data will not resolve the concerns that have been raised. Instead, this approach will seriously hamper innovation, make our economies less competitive, discourage investment and job creation, block access to services and increase costs. We rather recommend initiatives that aim at guaranteeing the same level of protection for the rights of European citizens, irrespective of the countries where their data are processed, while allowing for the flow of such data, as required in a global economy.

Data flows are necessary for all kinds of business activity and must be supported as a general principle, not as an exception.

* * *