Brussels, 10 May 2013

Cross Border Data Flows
An Imperative for all trading companies in a global world

ESF Position Paper[1]

ESF calls EU trade negotiators that any trade agreements should include binding provisions aiming at:

1. Allowing cross-border data flows processed for the provision of legitimate activities that are in compliance with the applicable legislation on data protection of both contracting parties;
2. Ensuring that cross-border data flows are not limited by a requirement of establishment of a local presence; with only few mutually agreed and well justified exceptions;
3. Allowing cross border data flows without requirement of locally based servers. The obligation to use local infrastructure or to establish a local presence should not be required as a condition of supplying data services. Preferential treatment to national suppliers should be prohibited in the use of local infrastructure, national spectrum, or orbital resources; and
4. Ensuring that local infrastructure used for conveyance of signals on electronic communications networks is made available to service suppliers under fully non-discriminatory terms and conditions.

The fast growing innovation in information and communication technology (ICT) is clearly one of the most dynamic elements in the development of the world economy in the last decades. This innovation has spilled over all economic sectors and has generated a large part of the economic growth and numerous jobs in the developed and emerging countries alike. This innovation has permitted the electronic provision of numerous ICT services that are now used by virtually all economic actors. They are particularly relevant for the functioning of the global value chain in manufacturing as well as services. Services, which provide or rely on electronic transfer of data in the normal course of daily business include business & professional services, financial & insurance services, information & communication services, education, entertainment &environmental services, retail, logistic and transport services.

The importance of the digital economy through the development of new technologies such as cloud computing and the internet of things, as enablers for the development of the whole economy, through the e-commerce, but also through nearly all activities of any companies is now well-recognised and praised by all economic actors and political decision makers.

The normal functioning of the digital economy requires the routine movement of large amounts of personal data, within the domestic economy, but also in this global world, across borders, including between the EU and third countries.

[1] *The European Services Forum (ESF) is a private sector trade association that represent the interests of the European services industry in International Trade Negotiations in Services & Investments. It comprises major European service companies and European service sector federations covering service sectors such as financial services, tourism, telecommunications, maritime transport, business and professional services, distribution, postal and express delivery, IT services, energy services and the audio-visual industry (see full list of members on the web-site: www.esf.be). It is estimated that ESF membership covers approximately 70% of Extra EU services exports and investments. ESF members employ more than 90 million workers, are present in more than 200 countries and provide services to hundreds of millions of consumers in Europe and around the world. The European Union is by far the largest exporter of international trade in services (26% of world share).*

The European Services Forum fully agrees with the need for the governments to accomplish the legitimate goals of both protecting and securing customers' information while fully complying with government requirements regarding citizens and companies' data and information privacy and security. However, ESF would like to encourage the governments to not set prohibitive or restrictive regulation for data protection that might have a negative effect on business as long as robust safeguards for the processing of that data are in place. ESF supports strong principles for protecting individuals' data, aimed at easing the flow of personal data across borders while still ensuring a high and consistent level of protection without loopholes or unnecessary complexity.

ESF and ESF Members are following closely the development of the proposal for a Regulation on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Many ESF Members have already expressed their views on this proposal and ESF reserves the right to provide comments on this specific legislative procedure in a separate position. This paper will focus on the international dimension of the digital economy and the need for a smooth cross border data flow in a globalised world. This paper will therefore also comment on the impact of the proposed GDPR[2] on the global dimension.

1. The need for harmonised cross border data flows' regimes in trade agreements

Given that trade is global and that data flows need to cross the borders to allow efficient global supply chain, ESF urges the European Union to ensure that the EU trade policy will be an instrument to set up new trade rules that allow companies of trade agreements parties to take full advantage of the enabling effect of the digital economy.

The European Union has already taken some important cross border services commitments[3] in its schedule of Commitments undertaken through the WTO GATS agreement in the Uruguay Round, as well as through the regional and bilateral free trade agreements. The European Services Forum takes note of these positive undertakings, but also reminds that those agreements are partly not up-to date anymore, in particular when it comes to ICT related services. A review of the relevant sections will be an important task for the forthcoming plurilateral services negotiations.

ESF also welcomes the **ICT principle on cross border information flow** approved by the European Union and United States in April 2011[4], which clearly states that "*Governments should not prevent service suppliers of other countries or customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in other countries*". Similarly, we take note of the EU to abide and spread out the fourth principle on **no requirement of local infrastructure**, which states that "*Governments should not require ICT service suppliers to use local infrastructure, or establish a local presence, as a condition of supplying services. In addition, governments should not give priority or preferential treatment to national suppliers of ICT services in the use of local infrastructure, national spectrum, or orbital resources*".

Nowadays, basically no international trade can be done without cross border data exchanges. It is therefore becoming imperative to adopt a comprehensive trade policy on this issue of cross-border

---

[2] *Please note that when talking about the GDPR – it applies to the EEA (European Economic Area), so this paper will often refers to EEA. Hoever, in terms of trade related aspects, EU is the relevant party as trade is outside the scope of the EEA agreement.*

[3] *Mode 1 of the GATS – "The supply of a service (a) from the territory of one Member into the territory of any other Member", GATS Article I. 2. (a); i.e. export of services that cross the borders without a commercial presence of the exporter in the recipient country.*

[4] *The European Commission and the US Government, under the framework of the Transatlantic Economic Council (TEC), have agreed on a set of ten fundamental principles for trade in information and communication technology (ICT) services. The EU and the US, in cooperation with other countries, will promote these principles worldwide in order to support the global development of ICT networks & services and allow service providers to compete for contracts with local incumbents on an equal footing.*

information flows, that should automatically be part of all on-going trade negotiations, either multilateral, plurilateral, regional or bilateral. We think in particular that cross-border data flow should be one of the horizontal disciplines to be included in the forthcoming plurilateral Trade in Services Agreement (TISA) negotiations in addition to being embedded into EU's updated template for Free Trade Agreements. We obviously have also in mind not only the EU-US Transatlantic Trade and Investment Partnership (TTIP) negotiations to be launched in the coming months, but also the negotiations with Japan and all others on-going FTA talks that the EU is currently running.

To this end, ESF would argue **that any trade agreements should include binding provisions** aiming at:

1. Allowing cross-border data flows processed for the provision of legitimate activities that are in compliance with the applicable legislation on data protection of both contracting parties;
2. Ensuring that cross-border data flows are not limited by a requirement of establishment of a local presence; with only few mutually agreed and well justified exceptions;
3. Allowing cross border data flows without requirement of locally based servers. The obligation to use local infrastructure or to establish a local presence should not be required as a condition of supplying data services. Preferential treatment to national suppliers should be prohibited in the use of local infrastructure, national spectrum, or orbital resources; and
4. Ensuring that local infrastructure used for conveyance of signals on electronic communications networks is made available to service suppliers under fully non-discriminatory terms and conditions.

To be efficient and well recognised by its interlocutors, this external aspect of the EU data protection policy must be coherent with the legislation adopted in the EEA single market. To this end, there is a clear **need to have a coordinated approach by the whole European institutions**. The European Services Forum urges the various bodies in charge of electronic communications and ICT services, data protection and trade policy to engage into a dialogue towards a comprehensive strategy on cross border data flows. In particular, experts and officials from DG Trade, from the Trade Policy Committee (TPC) of the European Council and from the International Trade Committee (INTA) of the European Parliament should also be consulted in the on-going discussions on date protection reform[5].

2. Towards global harmonisation of Data Protection legal regimes

Global companies operating worldwide frequently face varying obligations under data protection rules in different jurisdictions. This creates a confusing and non-harmonised patchwork of legislation that companies are confronted with and have to abide with, with sometime contradicting requirements. Indeed, in some jurisdictions, the rules are very strict and technical, while in others the requirements are more flexible (notably the OECD or APEC Guidelines).

With the advent of the e-commerce, information is flowing among companies (intra and extra company's flows) and between individuals and companies without regard to national borders. Companies are therefore advocating for international standards in data transfers across their global operations. They want simple, consistent and practical data protection standards that can be accepted and implemented in all jurisdictions. The aim is not to lower the standards of data protection but to provide similar data protection compliance regime to all data subjects wherever that subject is located.

[5] *In the current legislative debate on the GDPR in the European Parliament, many committees are consulted (Lead: LIBE – Opinion: EMPL, ITRE, IMCO, ECON & JURI), but INTA is not, despite the fact that this issue of cross border data flows will be discussed in the forthcoming FTAs and other international trade agreement like the plurilateral Trade in Services Agreement currently negotiated in Geneva.*

The European Services Forum calls for the EU to lead the work towards the setting up of international data protection's standards that should be compatible with EEA legislation, if it wants to avoid balkanisation of the digital economy. Such a harmonised and coherent data protection regime would provide greater certainty and clarity for the companies holding and processing the information while providing individual data subjects with confidence that their data privacy will be properly dealt with**.**

To this end, we would like to draw the attention on the on-going work of the OECD and APEC on this issue and we would like to strongly encourage the EU Commission to participate in this work, based on industry input.

One of the major inputs of the industry is a call to recognise the principle of accountability as a basic requirement to ensure consistency and responsibility in compliance with data privacy obligations. An **accountability-based system** requires data exporters to protect data or face sanctions for non-compliance. Companies that invest in comprehensive privacy policies, procedures such as Binding Corporate Rules, and standards should be allowed to process personal data freely across borders. This principle is already recognized by both APEC Privacy Framework and OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and we welcome that the new draft General data Protection Regulation has included specific provisions to exchange data on the basis of binding corporate rules.

To remain authoritative and influential on the global scene of data protection policy, the EU should **work together with its major counterparts** and contribute to the building of widely agreed international standards on data privacy.

3. International Data Transfers in the proposed EU regulation

Although this paper does not aim at providing comments on the whole European Commission Data Protection reform, there are some aspects of this reform that will have a direct impact on the international (non-EU) dimension of data transfers and must therefore be tackled in this paper.

Non-EU services providers, who target consumers in the EU – e.g. online services, – should apply the EU Data Protection rules in order for all businesses to compete on equal footing in the EEA and to provide a consistent protection to EU citizens. Otherwise, they would have a competitive advantage and therefore it will discriminate even further EU-based companies. It is an additional element that shows that there is a clear need to work with all data protection agencies on an international data transfer regime, that guarantees the effective protection of privacy at an international level as well as to ease the international flow of personal data, essential in a globalized world. This element needs to be taken into account when negotiating Trade Agreements.

Companies operating in the European Union are not allowed to send personal data to countries outside the European Economic Area unless there is a guarantee that it will receive adequate levels of protection. Such protection can either be at a country level (if the country's laws are considered to offer an adequate level of protection) or at an organizational level (where a multinational organization produces and documents its internal controls on personal data – see below). The EU legislation has an extra-territorial effect since it analyses the data protection regimes of other countries and, depending on this assessment, provides or not an **adequacy regimes** that will oblige or not the data exporter to abide by additional obligations. An adequacy decision is an acknowledgement that a given non-EU country ensures an adequate level of data privacy protection through its domestic law or/and international commitments.

ESF would **call for a significant improvement of the assessments procedure.** These assessments towards "adequacy decisions" should be made on a more transparent basis with explicit criteria, and in a short clear timeframe, to give better visibility to companies dealing with data from the assessed

countries. The status of the data, the derogations enabling transfers when a process has been found inadequate should notably be clarified.

One of the most famous examples of the adequacy regime is the "Safe Harbour Privacy Principles" that have been agreed between the EU and the U.S. and that allow US companies to register their certification if they meet the European Union requirements. But given the new obligations in the draft regulation (notably the explicit consent, sanctions and the right to be forgotten), it seems unavoidable that the Safe Harbour principles would have to be reviewed. We urge the authorities to work on this process as early as possible after the adoption of the regulation to ensure a smooth continuity of the regimes.

In the same spirit, there is also a **clear need to streamline and harmonise the notification and approval's requirements for Binding Corporate Rules (BCRs)** and Model Contractual Clauses (MCCs) that are in the EU legislation. The reform should introduce mechanisms that would reduce the bureaucracy and burden on companies while offering adequate levels of data protection. We welcome the recognition for the first time of a clear legal basis for BCRs and the extension of the use of the BCR to also cover data processors and within 'groups of companies', thus better reflecting the multiplicity of actors involved in data processing activities, especially in the framework of cloud computing. It should be clarified that global companies should be free to include only certain subsidiaries in their BCRs, depending on their needs and in keeping with the flexibility that BCRs are meant to provide. Similarly, we would encourage the European Commission to revise and improve standard contractual clauses that were reviewed in 2010.

Moreover, we also welcome the flexibility for international transfers of personal data in the absence of an adequacy decision from the European Commission. In particular, the proposed GDPR establishes the possibility of a transfer (or a set of transfers) of personal data, should this be necessary for the purposes of the legitimate interests pursued by the controller or the processor. Under the legitimate interest ground, cross border data flows become easier and less restrictive, thus allowing trading companies to proceed in such transfers and meet the realities of today's data driven society.

The proposed GDPR does not solve however some issues such as the need for further simplification for international transfers within a group of companies or the need for a mechanism for transfers between EEA based companies and non-group companies outside of the EU, which are very often business critical. An additional solution could be based on a combination of standard contractual clauses with a certification regime (such as an ISO certification) on a voluntary basis.

The European Services Forum believes that data exporters should remain responsible wherever processing takes place and have the tools necessary to assess risk and ensure compliance of data privacy. Our companies have clients and data subjects all over the world, inside and outside the EU. We call upon the European legislators to recognise the need to take into account the evolving nature of technology, like the growing advent of cloud computing. The current BCR system is currently too narrow in scope (applying only to intra-group transfers and to data-controllers) and too long and costly in its implementation. In this global world where data is exchanged at fast speed, companies need to be able to certify their handling of data on a worldwide basis, as long as adequate safeguards are in place for the fair processing of the data.

See Below the list of ESF Members supporting this Position Paper

LIST OF ESF MEMBERS

SUPPORTING THE ABOVE POSITION

- Architects' Council of Europe –ACE
- British Telecom Plc
- Bureau International des Producteurs et Intermédiaires d'Assurances – BIPAR
- BUSINESSEUROPE
- BUSINESSEUROPE WTO Working Group
- Deutsche Bank AG
- Deutsche Telekom AG
- DHL Worldwide Network SA
- DI – Confederation of Danish Industries
- Ecommerce Europe
- EK - Confederation of Finnish Industries
- Ernst & Young
- EuroCommerce
- European Association of Cooperative Banks – EACB
- European Banking Federation – FBE
- European Community Shipowners' Associations – ECSA
- European Express Association – EEA
- European Federation of Engineering and Consultancy Associations – EFCA
- European International Contractors – EIC
- European Public Telecom Network – ETNO
- European Savings Banks Group – ESBG
- European Satellite Operators Association – ESOA
- European Savings Banks Group – ESBG
- European Satellite Operators Association - ESOA
- Fédération des Experts Comptables Européens – FEE
- Fédération de l'Industrie Européenne de la Construction – FIEC
- Foreign Trade Association - FTA
- IBM Europe, Middle East & Africa
- Inmarsat
- Irish Business and Employers Confederation
- KPMG
- Law Society of England & Wales
- Mouvement des entreprises de France – MEDEF
- Oracle Europe, Middle East & Africa
- Orange
- Siemens AG.
- Standard Chartered Bank
- Svenskt Näringsliv (Confederation of Swedish Enterprise)
- Tata Consulting Services
- Telefónica SA
- Telenor Group
- The CityUK
- Thomson-Reuters
- Zurich Financial Services

• Avenue de Cortenbergh, 168 • B – 1000 - Brussels • Belgium • TVA BE 863.418.279
Email: esf@esf.be • Tel : +32-2-230 75 14 • Fax : +32-2-230 61 68 • www.esf.be