ERICSSON

# EU FREE TRADE AGREEMENT PROPOSITION

## ALLOWING DATA FLOWS AND RESPECTING DATA PRIVACY

December 2016

# INDEX

# INTRODUCTION

## Benefits

The following proposal has at least two potential beneficial outcomes.

Firstly, setting down both the principle of free data flows and basic provisions for data protection would provide **greater predictability and transparency for economic operators in how data transfers are to be regulated.**

Secondly, the proposed provisions would arguably st**rengthen the application and extension of the EU's data privacy rules** including the General Data Protection Regulation ("**GDPR**"), as explained in a recent report by the law firm Mannheimer Swartling. Using Free Trade Agreements ("**FTAs**") to promote the principle of free data flows and to establish mutually-agreed rules for data transfers would help safeguard the EU's data privacy rules against possible challenges under global trade rules of the World Trade Organization ("**WTO**").

## Purpose

This proposal contains a standard EU position on data flows, which may be used in any bilateral or multilateral FTA negotiation. The aim of this proposed EU position is to consolidate and to satisfy two strong and potentially conflicting interests: on the one hand, allowing a principle of free data flows between the EU and other countries, and on the other hand, ensuring a high level of data privacy protection in such data flows.

## Scope

This proposal focuses on these two interests only. Ericsson envisages that other questions and interests may arise in FTA negotiations, however these are beyond the scope of this proposal.

The proposal firstly **establishes a basic principle of allowing data transfers** (data flows). To ensure the effective free flow of data in practice, the proposal also contains mutual commitments to refrain from i) localisation requirements and ii) mandatory disclosure of source code, as such types of *domestic regulation* inhibit the free flow of data.

The text also introduces data privacy protection as a pre-condition for data flows, based on a principle that the parties will agree, through regulatory cooperation, on mutually-satisfactory standards of data protection.

## Structure

A data transfer is *per se* neither a physical good nor a service (even if data transfers sometimes are linked to the supply of a good or a service). The principle of free data flows should therefore stand on its own, rather than be a secondary obligation under provisions related to goods or services. EU FTAs commonly feature sections on electronic commerce − which cater well for provisions on data transfers. Other common sections, e.g. on regulatory cooperation and general exceptions, should then cross-refer to the section on electronic commerce[1].

The proposal is followed by a reading guide explaining the background and reasoning.

# 1. MAIN PRINCIPLES: ALLOWS CROSS-BORDER DATA FLOWS

## (electronic transmission of information)

The following proposed articles are intended for a section on electronic commerce.

**Article 1**

**Conditions for free cross-border electronic transmission of information**

1. The Parties agree to allow cross-border electronic transmissions of information, including personal data, that is undertaken by a natural or legal person of a Party as part of that person's economic activity and provided that when transmissions contain personal data, that personal data is protected according to mutually-agreed regulatory cooperation measures as set out in Article 2.

2. The Parties agree that when the electronic transmission of information is part of the provision of a service, within the meaning of [section on services] (cross-border supply of services), the obligations set out there in shall extend to any measures affecting such cross-border electronic transmissions of information.

3. Nothing in this article shall prevent a Party from adopting or enforcing measures under a General Exception [in Article X].

**Article 2**

**Regulatory compatibility for the protection of personal data**

1. Regulatory cooperation activities will be conducted between the relevant regulatory bodies of both Parties, to achieve mutually-agreed regulatory compatibility for the protection of personal data in cross-border electronic transmissions. Regulatory compatibility may be achieved through different means, including:

a) common principles on data protection, guidelines, or codes of conduct;

b) mutual recognition of equivalence or harmonisation of data protection regulations in whole or in part;

c) mutual recognition or reliance on each other's implementing, monitoring or enforcement tools; or,

d) mutually-agreed exceptions for defined types of data transfers, including where there is a legitimate interest of the natural or legal person transferring the data and the purpose of the transfer is not to access or process the personal data contained therein.

**2. The Parties shall ensure that any control or approval procedures that are part of mutually-agreed regulatory compatibility under this Article:**

a) are undertaken and completed without undue delay;

b) adhere to published processing periods or to anticipated processing periods that are communicated to the applicant upon request; and,

c) are based on information requirements that are limited to what is necessary for appropriate control or approval procedures.

**Article 3**

**Customs duties**

The Parties agree that any electronic transmissions of information covered by this Agreement, whether performed as part of a covered service or as a stand-alone transmission, shall not be subject to customs duties.

**Article 4**

**Prohibition on localisation requirements and disclosure of source code**

1. The Parties shall not require the use of local computing facilities in a Party's territory as a condition for conducting economic activity in that territory.

2. The Parties shall not require the disclosure of source code of software owned by a natural or legal person of a Party, as a condition for the sale or use of such software, or of products containing such software, in its territory.

3. Nothing in this article shall prevent a Party from adopting or enforcing measures under a General Exception in [Article X].

# 2. ADDITIONAL INSERTS TO ENSURE COHERENCY

The proposed text below relates to the section on regulatory cooperation. Usually this section includes provisions setting out the scope of the FTA, which then should include a cross-reference to the specific provisions on protection of personal data in the section on electronic commerce. The proposal below is based on the EU's proposed negotiating text in the Transatlantic Trade and Investment Partnership ("**TTIP**").

The EU's FTA provisions on general exceptions usually mirror GATS Article XIV very closely. If the FTA departs from the standard wording, as is the case in the EU's proposed negotiating text in the TTIP, Ericsson recommends safeguarding that cross-border transmissions are also protected from disguised restrictions.

**Regulatory Cooperation**

**Article X**

The provisions of this section shall apply to:

a) Cooperation covered by specific or sectorial provisions concerning goods and services in this Agreement [to be identified] [when identifying sectors, regulatory cooperation for data protection in electronic commerce is to be included]

(x) Regulatory cooperation for the protection of personal data in cross-border transmissions of information shall follow the specific provisions set out in [Article 2, Section on Electronic Commerce].

General Exception

Article X

…or a disguised restriction on establishment of enterprises, the operation of investments, cross-border supply of services or the cross-border transmission of information, nothing…[amendment underlined]

# READING GUIDE

## 1. Preliminary note regarding terminology for data flows

The term "data flows" is customarily used to identify large volumes of information moved from one location to another. In FTAs, terms such as "electronic transfers" or "transmission" are used. The term "information" is also used synonymously with "data".

In the proposal above, the term "electronic transmission of information" is used instead of "data flows", which mirrors the EU's negotiating text in TTIP.

## 2. Main principle: allowing cross-border data flows

Recent FTAs have generally included a section on electronic commerce with provisions related to electronic commerce in general. However, data flows as such (electronic transmission of information) are not specifically included in any EU FTAs. The US Trans-Pacific Partnership ("**TPP**") includes such provisions, which may serve as a point of reference.

### 2.1 Allowing electronic transmission (data flows) and protecting personal data

The main purpose of this proposal is to introduce a general principle that electronic transmissions are allowed *per se* (Article 1.1), subject to two conditions. The first condition is that the transmission is part of an economic activity. This is similar to the scope of the TPP and is consistent with the scope of current EU laws on data privacy.

The second condition relates specifically to those transmissions that contain personal data. Such **personal data must be awarded protection** "according to mutually-agreed regulatory measures". This wording is intended to link back to a general section on regulatory cooperation. In the EU's negotiating position in TTIP, this section lists a high level of **protection of personal data and cybersecurity** as one of its objectives[2]. It should not be controversial, therefore, to introduce a clause stating that the Parties should cooperate to ensure protection of personal data, as this would merely reflect an existing priority objective of the EU. This priority is featured, for example, in the EU

- Canada Comprehensive Economic Trade Agreement ("**CETA**"), which sets out the importance of a dialogue on data protection in electronic commerce[3] and in the EU - US Privacy Shield Framework (the "Privacy Shield").

Further, Article 2 lists specific types of regulatory cooperation activities and measures that would allow the authorities of each Party to agree on regulatory compatibility. This list is not exhaustive and includes general principles, code of conduct, mutual recognition, and reliance on each other's enforcement tools. The list mirrors the EU's TTIP negotiation position on regulatory cooperation.

The FTA itself would not regulate what the level of protection should be, but defer on this question to the respective authorities. This allows flexibility for the respective authorities in the EU and the other contracting Parties to agree on how to achieve a sufficiently high level of protection for personal data. The proposed text contains broad references to several types of measures, which could cover the measures already undertaken under the Privacy Shield, as well as in the EU Commission's adequacy decision on the Privacy Shield[4].

Until regulatory compatibility is agreed and in place, transmissions containing personal data would not benefit from the principle of free data flows in Article 1. However, transmissions that do not contain personal data would benefit straight away from the principle of free data flows, without the need to agree on regulatory cooperation. This structure would serve to delineate between data flows containing personal data and data flows not containing personal data. It would thus arguably make restrictions on data flows, for data privacy reasons, more proportionate and compatible with the necessity requirement under GATS Article XIV.

As well as calling for mutually-agreed regulatory compatibility standards to govern personal data flows, the proposal also reflects that not all data transfers containing personal data are equal, and may therefore be treated differently. Under Article 2.1(d), the proposal gives the authorities the possibility to agree on exceptions for certain defined types of data transfers which may contain personal data, but where there is a legitimate interest in transferring the data and the purpose is not to access or process the personal data. Such an exception would be particularly useful when providing business to business maintenance services for instance, where data is temporarily accessed from, or transferred to, countries where data specialists are located.

## 2.2 Transparent and predictable control and approval procedures

Article 2.2 introduces an obligation for the Parties to ensure that any control or approval procedures are transparent and predictable. The purpose of this sub-article is to ensure that if the Parties agree, under the framework of regulatory compatibility, for example, that data transfers containing personal data must undergo control or approval procedures before being transferred to the other Party, that such procedures should be completed without "undue delay" and according to published/communicated time lines. Also, the information requested from the authorities for such a procedure must be necessary (as well as proportional and reasonable) in relation to the purpose of the approval.

This language is borrowed from Article 8 and Annex C of the WTO Agreement on the Application of Sanitary and Phytosanitary Measures ("**SPS Agreement**"). Recently, these provisions have been interpreted by several WTO Panels,[5] which could serve as a source of interpretation when assessing lead time and information requirements for approving data transfers containing personal data.

## 2.3 Clarifying obligations for transmissions linked to services

In the EU's negotiating position in the TTIP, the EU implies that the transmission of information **(data flows)** should be treated as a service, and in other cases, there is no mention of how data transmissions are to be treated.[6] As set out in the report by Mannheimer Swartling, data transmission should in any event benefit implicitly from a Party's WTO commitments on services, when the data transmission is linked to the provision of such a covered service.

The lack of clarity on this matter, however, would likely create difficulties in determining if a transmission of information is connected to a service, and if so, to which covered service it would be connected. For example, the EU's negotiation position in the TTIP covers only certain services associated with the provision of cloud computing. This would likely cause uncertainty for operators that make use of cloud services in their own activity (e.g. companies storing customers data in a cloud hosted by a third party). Such operators may **find it difficult to determine whether a transmission of information would be covered**, e.g. whether data in the cloud would be considered part of a computer service**, another service covered by a TTIP-commitment, or actually a service outside of the scope of TTIP**.[7] Furthermore, viewing the transmission of information as an auxiliary element to services makes it more difficult to introduce broader horizontal provisions on data protection in such transmission of information.

The proposed Articles 1.1 and 1.2 would provide greater certainty to operators, eliminating the need to link the transmission to a specific service. In other words, operators would be able to rely on one main principle, rather than having to first define what type of service the data is associated with. The transmission of data would be allowed *per se*, provided that the personal data is protected. This would arguably achieve greater horizontal protection for data privacy (for all types of information transmissions generally, and not only those directly linked to a service), thereby better serving EU policy objectives than by treating the transmission of information as an auxiliary element to a specific service.

Furthermore, Article 1.2 ensures that, in any event, if an transmission is linked to a covered service, then the commitments *vis-a-vis* that service also extends to the transmission.

## 2.4 Reference to General Exception

The proposed Article 1.3, refers to a Party's option of applying a general exception, which usually is identical to GATS Article XIV. If the EU would want to adopt measures restricting electronic transmissions for reasons other than data protection, that option remains open, as long as any measures would be compatible with the conditions in GATS Article XIV as interpreted by the WTO.

## 3. Preventing localisation requirements and the disclosure of source code

The two commitments - to refrain from imposing localisation requirements and to refrain from imposing rules on disclosing source code - have been placed together under the proposed Article 4. There is also a reference to the general exception section, which allows a Party to depart from these commitments. Any such measures would need to be compatible with the conditions in GATS Article XIV as interpreted by the WTO.

**The purpose of these two provisions is to prevent certain types of domestic regulations that may effectively or indirectly prevent the free flow of data.** For example, a rule requiring the disclosure of sources code is a practical barrier to free data flows as it imposes a strong disincentive for operators to provide any type of computer services in the country.

## 4. Additional inserts to ensure coherency

EU FTAs usually include a section on regulatory cooperation. To ensure coherency with the main proposal for electronic commerce, it is important that the section on regulatory cooperation contains a reference to the specific provisions on data protection in the section on electronic commerce. **The specific provisions contained in the section on electronic commerce would thus prevail over any conflicting provisions in the general section**. This affords greater certainty and flexibility for the authorities to agree on specific compatibility standards for data transmissions.

The proposed change to the section on general exceptions, stems from the EU's negotiation position in the TTIP. These provisions usually mirror GATS Article XIV very closely. If the FTA departs from the standard wording, as is the case in the EU's proposed negotiating position in the TTIP, Ericsson proposes to ensure that also cross-border transmissions are protected from disguised restrictions. Thus, if a general exception is tailored to mirror the different sections of the FTA (i.e. to list what is included rather than a broad reference to trade), **it is important to ensure that data flows benefit from the same level of protection against disguised restrictions**.[8]

# REFERENCES


1. For example, under the TTIP, we would propose to introduce these texts under Chapter VI - Electronic Commerce and Chapter VII - Exceptions, both under the Trade in Services, Investment and E-Commerce title, as well as under the Regulatory Cooperation title.
2. See the EU's negotiating position in TTIP, Article x1.(b) under Regulatory Cooperation.
3. See CETA, Article 16.6.1(d)
4. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 2016, p.1.
5. See, e.g. WTO Panel Report *Russian Federation - Measures on the Importation of Live Pigs, Pork and Other Pig Products from the European Union*, WT/DS475/R, which includes references to the Panel Report in, *European Communities – Measures Affecting the Approval and Marketing of Biotech Products,* WT/DS291/R, Add.1 to Add.9 and Corr.1 / WT/DS292/R, Add.1 to Add.9 and Corr.1 / WT/DS293/R, Add.1 to Add.9 and Corr.1, adopted 21 November 2006, and the Panel Report in *United States – Measures Affecting the Importation of Animals, Meat and Other Animal Products from Argentina*, WT/DS447/R.
6. See the EU's negotiating position in TTIP, Article 6-3 under Electronic Commerce. However, in the recently concluded FTA with Vietnam, transfers of data are not mentioned at all in the section on electronic commerce.
7. The EU's negotiation position in the TTIP, Article 5-13 in Section III – Computer Services specifies that computer services are covered (CPC 84), and that this can include under indent 3 (a) consulting, strategy, analysis, planning, etc.; and under indent 3 (c) data processing, data storage, data hosting or database services. These provisions would cover cloud services. Any transmission of information (data flows) linked to these services, therefore, would presumably be covered by commitments for the associated covered service. However, indent 4 distinguishes between the covered services (e.g. web-hosting or application hosting) and its content (e.g. data or information) or core service that is being delivered electronically. Such services or transmissions of information connected with these services are therefore not covered by Article 5-13 (but possibly other covered services).
8. CETA contains a simple and broad reference to "*disguised restriction on international trade*", which would likely include the provisions on data flows.

Ericsson is the driving force behind the Networked Society– a world leader in communications technolocy and services. Our long-term relationships with every major telecom operator in the world allow people, business and society to fulfill their potential and create a more sustainable future.

Our services, software and infrastructure– especially in mobility, broadband and the cloud– are enabling the telecom industry and other sectors to do better business, increase effciency, improve the user experience and capture new opportunities.

With apporximately 115,000 professionals and customers in 180 countries, we combine global scale with technology and services leadership. We support networks that connect more than 2.5 billion subscribers. Forty percent of the world's mobile traffice is carried over Ericsson networks. And our investments in research and development ensure that our soluitions—and our customers– stay in front.



LM Ericsson AB

SE– 126 25 Stockholm, Sweden

Telephone +46 10 719 00 00

Fax +46 8 18 40 85

www.ericsson.com