

Data flows in TTIP



Introduction

The negotiations between the U.S. and the EU on the Transatlantic Trade and Investment Partnership (TTIP) will address e-commerce and transatlantic data flows. The European Consumer Organisation (BEUC) is concerned that including data flows will result in a significant weakening of consumers' fundamental rights to privacy and to the protection of personal data. It is impossible to address these issues when the data protection regimes in the US and EU are starkly different.

Negotiators' claims that TTIP will not touch upon issues of privacy or data protection have not been substantiated. Data flows by definition include the flow of personal data. This is even more the case in the context of e-commerce, where a consumer's personal data needs to be processed to conclude an online sale.

There are currently no comprehensive data protection laws in the United States. In order to transfer personal data to the US, American companies voluntarily commit to apply European standards under the Safe Harbour Act. This process is largely ineffective, as has been demonstrated by the ongoing [review of Safe Harbour](#).

The EU and the US should discuss common data privacy standards, but they should do so outside of the proposed TTIP negotiations considering that the data protection regimes in the US and EU are thoroughly different.

What is on the table?

The American side is pushing for interoperability between data protection rules on both sides of the Atlantic, which boils down to undermining European data protection standards. The US draft for the e-commerce section of TTIP reportedly includes two crucial points: the principle of "interoperability" of European and US data protection rules, and a ban on "localization"¹.

In parallel to TTIP, negotiations on a new plurilateral Trade in Services Agreement (TiSA) are seeking to open markets in areas such as financial services, telecoms and e-commerce. According to a [leaked](#) draft, TiSA would allow financial institutions to freely transfer data, including personal data, from one country to another. Another leaked document, a draft of the TiSA "Electronic Commerce and Telecommunications Services Annex"², contains provisions that would ban restrictions on cross-border information flows and localisation requirements for information and communication technology (ICT) service providers. Another provision would rule out any conditions on the transfer of personal data to third countries, as is currently the case under EU data protection laws.

1. Data localisation refers to rules requiring data storage and processing to take place within a specific geographical boundary. EU data protection rules require that personal data in principle may only be processed in Europe or in those countries declared by a European Commission decision to offer an adequate level of protection.

2. <https://data.awp.is/data/filtrala/15/tisa.cleaned.pdf>

Data flows in TTIP



What does it mean for EU citizens/consumers?

- Personal information, including name, ID numbers, IP address, emails, contacts, will be transferred to the US without any safeguards.
- Data collected by US companies about European consumers will be accessible to US law enforcement authorities once transferred to the US without any legal safeguards in terms of transparency, proportionality or redress.
- Once personal data has been transferred to the US, it can be transferred on to anywhere in the world on the basis of bilateral trade agreements signed by the US with third countries, which do not necessarily meet the European privacy standards.
- Including data flows in TTIP risks delaying the much needed reform of the EU Data Protection framework which seeks to strengthen the rights of Europeans and which will oblige US companies to comply with EU legislation.

Our recommendations

- The EU should introduce a general exception ('horizontal clause') in TTIP that indicates that EU data protection rules apply to all products and services offered to EU consumers.
- The EU should refrain from negotiating personal data flows and data protection rules under TTIP. If the Commission would decide otherwise, it should at least wait for the approval of the data protection reform package by the European Parliament and the Member States.
- The EU should not accept that privacy and data are barriers to trade; EU data protection legislation cannot be deemed an 'arbitrary or unjustifiable discrimination' to transatlantic trade.
- The EU should ensure that any provisions in the agreement which touch upon the localisation of data processing equipment must not undermine EU rules on data transfers, which prohibit the processing of such data in third countries that do not meet the EU adequacy standard.

Rue d'Arlon 8 0
B -1 04 0 Brussels
Tel +32 (0)2 743 15 90
www.beuc.eu
@beuc

BEUC-X-2015-073

NOTE: In this [position statement](#) and [blog post](#) we describe in more detail how TTIP could benefit consumers and what needs to happen to prevent detriment to consumer safeguards.



This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).