SWP Comments

Stiftung
Wissenschaft und
Politik

German Institute
for International and
Security Affairs

# European Union Data Protection and External Trade

## Having the Best of Both Worlds?

*Annegret Bendiek and Evita Schmieg*

**The trade in digital technology and services has become an absolutely central element of international economic relations. A substantial part of this trade is associated with the transfer of data, some of it personal, and many of the new products and services emerging in connection with the internet exhibit new characteristics of relevance for data protection. A significant need for regulation has thus arisen, requiring closer cooperation between experts for trade law, data protection, and information and communication technology (ICT). This applies above all to the current negotiations on the Transatlantic Trade and Investment Partnership (TTIP) and to the new agreement on transatlantic data transfer (EU-US Privacy Shield).**

In matter digital, the international trade system and the regulatory efforts of individual states are lagging behind technical developments. The European Court of Justice and the European Commission have recently drawn red lines for internet companies operating internationally, but these have yet to be operationalised in legislation. The European Union's General Data Protection Regulation (GDPR) serves as the basis for transatlantic arrangements such as the EU-US Privacy Shield. At the same time the Union is negotiating with twenty-three other parties over a Trade in Services Agreement (TiSA) and with the United States about creating the world's largest economic space (TTIP). While German civil society became especially critical of TTIP in the wake of the NSA revelations, data protection is not in fact part of the TTIP talks. In October 2015 the Court of Justice overturned the Commission's Safe-Harbour Decision, which had regulated data transfer between EU member-states and the United States since July 2000. In early February 2016 the European Union and the United States agreed to replace Safe Harbour with the EU-US Privacy Shield.

## The Significance of Trade in Data

The growth of the internet has enormously expanded the importance of data transfer and the trade in services involving data protection:

*Dr. Annegret Bendiek is a Senior Associate in SWP's EU/Europe Division*
*Dr. Evita Schmieg is an Associate in SWP's EU/Europe Division*

- as a side-effect of the use of digital services (for example data transfer involved in using digital insurance services);
- by multinationals managing decentralised production in global value chains;
- in communication;
- in gathering user feedback for product development;
- in individual and in-house cooperation on research and development;
- as trade in data itself (such as consulting services, software, licensing of intellectual property rights, sale of statistics on use of internet services).

Today data is also generated by machines (including jet engines, lifts and cars) whose export thus implies data transactions in the service sector, for example as the basis for repair and maintenance work. The rules applied to such data will shape the provision of this kind of after-sales services: retaining it will enable an exporter to conduct maintenance work as a service export. Using and analysing the data generated and exchanged by digitally networked products such as smartphones and smartwatches in the "internet of things" requires free international exchange. The idea that consumers automatically approve the use and processing of their data is problematic. In reality, they often lack the IT skills required to apply privacy mechanisms and their interest in using the services on offer outweighs their interest in data protection. Data privacy concerns differ widely between societies; German consumers in particular are often very concerned to see their data better protected.

Digital services such as online consulting are becoming increasingly important. They already represent more than 50 percent of transatlantic service exports (United States 72 percent, European Union 63 percent). And they supply important production inputs for export goods. So significant sectors of industry are interested in exporting these products, as well as improving their access to imports that help them to lower their costs and improve their competitiveness. According to the United States International Trade Commission (USITC), the internet reduces average trading costs by 26 percent. Especially in developing countries the market for digital services is set to explode. Large parts of the world will join the internet using mobile devices, 54 percent of which will be "smart" by 2018 (up from 21 percent in 2013). Growing middle classes, whose size in Asia is heading to double by 2020, underline the great potential of online commerce.

## International Trade Agreements

Trade in services is regulated by the WTO's General Agreement on Trade in Services (GATS) of 1995, while a separate Information Technology Agreement abolishes tariffs on listed IT products. GATS involves general duties: under the most-favoured-nation principle all trading partners must be treated equally. And there are also rules on transparency. Liberalisation of trade in services is achieved through specific obligations for market access and national treatment, under which foreign service providers are granted the same treatment as their domestic counterparts. The liberalisation duties of individual WTO members are listed in so-called schedules.

GATS distinguishes four modes of supply of trade in services. Although numerous electronic services did not yet exist when GATS came into force, many are nonetheless covered by the GATS classification. Certain services can be provided both digitally and by other methods.

In 1996 seventy-nine WTO member-states concluded the Information Technology Agreement (ITA), abolishing tariffs on IT products such as computers, telecommunications equipment and semiconductors. But the ITA does not apply to services and contains no arrangements for data protection. All it does is broaden the spectrum covered by the WTO's liberalisation of trade, and it remains in all respects subject to WTO rules. After seventeen rounds of talks between the now fifty-four parties, trade liberalisation for an additional 201 IT

products was approved at the WTO ministerial conference in Nairobi in December 2015. The annual volume of trade in these products amounts to more than $1.3 trillion, and today represents about 7 percent of global trade.

The trade in data – in its own right or contained in other goods – is especially relevant from the data protection perspective. As a rule provision of digital services is not only associated with data transfers, but frequently also leads to the accumulation of large amounts of data (big data), which are economically attractive in themselves. For example sports watches gather millions of users' personal health data, whose aggregation represents an attractive source of information for the pharmaceuticals industry. Consequently, many aspects of trade in digital services touch on questions of data protection in dimensions that were inconceivable when the General Agreement on Tariffs and Trade (GATT) and GATS were drawn up (in 1947 and 1995 respectively). Today coordination of the various national data storage regimes is rudimentary or non-existent, and their relationship to international trade law is unclarified. The exceptions laid out in GATT and GATS form the legal basis for data protection rules.

- GATS Article III permits parties to keep information confidential in specific circumstances such as public interest;
- GATS Article XIV (General Exceptions) underlines the right of parties to adopt and enforce laws and regulations. This also applies to the protection of privacy in relation to the processing and dissemination of personal data.

The GATS Annex on Financial Services, section 2 (Domestic Regulation) specifies that parties are under no obligation to reveal information relating to individuals' business bank and accounts, or to confidential and other information in the possession of public entities.

## Data Protection in the Trade in Services Agreement

GATS created the basis for a further liberalisation of trade in services, which was originally to take place at the multilateral level. However, not all the parties were interested in further opening their service sectors. Currently, as a result, only plurilateral talks on a Trade in Services Agreement (TiSA) are being conducted under the auspices of the WTO. The European Union is negotiating on new principles for domestic regulation of ICT services (including cross-border data transfers), electronic commerce and computer-related services.

In relation to data protection, the European Commission emphasises that TiSA will contain the same safeguards as GATS. At the same time, it argues that the data transfer rules discussed for TiSA are inspired by similar provisions in existing free trade agreements, for example with South Korea. Article 7.43 of the latter agreement explicitly states that both parties should develop appropriate privacy protection rules, especially in relation to the transfer of personal data. As such, the South Korea FTA goes further than previous exceptions, regarding the proposed rules not as possible exemptions from free trade, but stressing the need to develop adequate safeguards in the first place. However, critics fear that the United States has already asserted its own diverging interests in the TiSA talks, and that TiSA will provide for free data transfer between its signatories.

## Data Protection in the TTIP Talks

The European Union is also negotiating in bilateral and regional contexts. For example, its mandate for the transatlantic free trade agreement TTIP also seeks a liberalisation of the service sector. TTIP is expected to have considerable potential repercussions on data protection matters. Here the different regulatory histories, economic situations and social preferences of the European Union and the United States lead to diverging positions. In view of the rapidly growing

role of IT goods and services mentioned in the introduction, the United States possesses a strong interest in free international exchange of data. But so do important parts of the European economy. Thilo Weichert of the Data Protection Centre in Schleswig-Holstein points out that talks in connection with "computer services" touch on practically all commercially used personal data. Data protection experts are very worried that TTIP will include rules that make data protection difficult or impossible in the European Union.

The Commission's mandate for TTIP underlines the right of the European Union and its member-states to regulate. The Union is therefore seeking to include an explicit right to take measures to achieve legitimate domestic and European policy goals to preserve national and European security interests. The section on services refers to the GATS general exceptions.

As already mentioned, the privacy questions regulated in the successor to the Safe Harbour agreement are not under discussion in the TTIP framework. Fundamentally, it is assumed that anchoring the GATS exceptions in new free trade agreements will offer adequate safeguards and policy space.

## The Development of Data Protection in Europe

After the OECD issued its non-binding Privacy Guidelines in 1980, the Council of Europe adopted the first legally binding Convention on Data Protection in 1981. The EU Data Protection Directive adopted in 1995 is still in place. It pursues two objectives of equal importance: "to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" and to ensure the "free flow of personal data between Member States". A Directive on privacy and electronic communications (ePrivacy Directive) followed in 2002, supplemented in 2009 with a cookie law to protect personal data generated in the form of cookies when using the internet.

Following Edward Snowden's revelations about the extent of NSA eavesdropping, the Facebook critic Maximilian Schrems took Facebook Ireland to court in June 2013. This led to the groundbreaking Court of Justice rulings of April 2014 on data retention and May 2014 on the "right to be forgotten", and set in motion a review of all EU rules relating to data protection and security. The Court of Justice's Safe Harbour ruling of October 2015 demanded further reforms. In mid-December 2015 the European Parliament, the Council of Ministers and the Commission agreed on a new General Data Protection Regulation (GDPR), which the European Parliament's committee on civil liberties, justice and home affairs approved by a large majority: 48 yes to four no votes and four abstentions. The Council of Ministers and the Parliament's plenary still have to pass the measure. Assuming they do, the first comprehensive reform of the EU data protection legislation of 1995 will come into force in 2018, to be immediately applied in national law. The Regulation applies to the entirety of the private and public spheres, excepting only the police and the judicial system, for which a new data protection directive was negotiated simultaneously.

## The General Data Protection Regulation

The GDPR will for the first time institute harmonised, binding data protection throughout the European Union, and is intended to avoid member-states competing to offer the weakest protections. "European law on European soil" is the Commission's motto. The new arrangements will require internet companies to obtain users' explicit consent if they wish to make use of their data. Users will also obtain the right to have stored information deleted (the right to be forgotten) and to take their data from one provider to the next (portability). Companies will have to supply products with data-protection-friendly default settings (privacy by design

and by default). And new data protection and security requirements will promote IT products whose technological configuration facilitates the protection of private data.

Firms from third states will also have to obey the new European rules, with violations subject to fines of up to 4 percent of annual turnover. In future, consumers wishing to lodge complaints against providers in other EU member-states will be able to do so in their own language through the relevant agency in their own country.

Data protection authorities are fulfilling an increasingly important regulatory and complaint-handling role, monitoring how personal data is used in the information society and imposing sanctions as necessary. In two verdicts (2010 and 2012) the European Court of Justice has emphasised the need for "complete independence" of data protection authorities in order to curtail the influence of third parties.

Certain aspects of the GDPR have attracted criticism. In the European Union data processing is tied to a defined purpose that limits its application, whereas the principle of necessity and limitation ("Erforderlichkeits- und Zweckbindungsprinzip") is unknown in the United States. The proposed limitations fundamentally contradict the business logic of fast-growing online platforms like Alibaba and ebay, while big data systematically subverts the concept given that the whole point of gathering and analysing enormous quantities of data is to use it for many different purposes, rather than repeatedly for the same purpose. In fact it is frequently statistical analysis of big data that generates new possibilities for using personal data in the first place.

The compromise reached for the GDPR provides exceptions for research, permitting pseudonymised data to be used for commercial research purposes. For example, administrative data is highly relevant for labour market research. Under the new arrangements there must be clear indications of consent for every piece of research. Yet tying declarations of consent to narrow criteria will hamper empirical research, which already has to contend with a lack of willingness to participate.

There has also been criticism of the possibilities for US and European security and intelligence services to access data stored in all the different EU states, whose availability is governed by national intelligence service legislation. These possibilities remain and will continue to contradict the harmonised EU data protection legislation. Although the GDPR reform package also includes a Data Protection Directive to harmonise the legal framework for the police and criminal justice sector across the European Union, this does not involve any transatlantic understanding on cooperation between intelligence services. Even the umbrella agreement on data protection for law enforcement purposes will not solve this problem.

## The Safe Harbour Agreement and the EU-US Privacy Shield

The Safe-Harbour Agreement was adopted in 2000, applying throughout the United States and the European Union. It was designed to ensure that US companies give adequate protection to European users' privacy when they process their data stateside. De facto, although not de jure, this was a decision by the Commission, in which it classified companies that agreed to observe particular data protection standards and submit to controls by the US Federal Trade Commission (FTC) as safe harbours. FTC Commissioner Julie Brill pointed out that in the fifteen years of its existence, just four reports of violations had been received from European data protection authorities, while altogether 4,400 US companies had registered on the basis of the agreement. During the same period, she said, the FTC had investigated numerous violations and initiated legal action in 39 cases, including against Facebook. However, the small number of legally relevant cases could also imply weaknesses in the effectiveness of Safe Harbour.

In October 2015 the European Court of Justice ruled that this arrangement for

commercial exchange of data between the United States and the European Union was invalid, following a complaint brought by the Austrian data activist Maximilian Schrems. The Court based its verdict on the Treaty of Lisbon and the EU's Charter of Fundamental Rights, which it said had granted "respect for privacy and family life" and "protection of personal data" the status of fundamental rights. The Court singled out US government access to European users' data for particular criticism.

The EU data protection authorities gave the Commission until the end of January 2016 to negotiate a new agreement. At the beginning of February the European Union and the United States agreed a new arrangement for data exchange between the two economic areas: the EU-US Privacy Shield. Under the agreement, the US Department of Commerce will monitor US companies processing data from Europe. Those that fall short of the standards will be fined or removed from the list. In other words, the US side agreed to regulation conducted by its own judicial and security organs. The two partners will review the agreement's implementation annually. Anyone who believes their data privacy rights have been violated on account of US national security interests will be able to turn to an ombudsman operating independently of the US security agencies. EU law demands a legal guarantee on this point. In case of conflict there will be a free mediation process.

Data retention represents another problem. The United States has pointed out that the amended USA Freedom Act permits general and blanket data retention only where it serves purposes relevant to criminal investigations. However, the American legislation applies only to investigations against Americans conducted within the United States. The Commission is relying on the United States granting EU citizens direct access to US courts to take action against misuse of their data. The agreement presupposes close cooperation between European data protection authorities and their US counterparts, especially the FTC. In March the Commission has published the legal foundations, EU data protection experts will be able to judge Privacy Shield against the Court of Justice's requirements before the EU states vote on the agreement.

Legal insecurity will persist in the medium term. The Court of Justice set out very strict requirements for correct implementation of an EU-US Privacy Shield. Many observers share the opinion of Emma Peters from the law faculty at the Humboldt University in Berlin, who argues that the Court's Schrems ruling was rash. As a result, she says, the Court is demanding that the United States guarantee safeguards for the data of EU citizens that the Union itself cannot demand of its own member-states, and that they in turn do not grant to US citizens either (JUWiss-Blog, 14 October 2015).

## Conclusions

European data protection will strongly influence future transatlantic data transfer. While TTIP is negotiated separately, the European Union's diverse data protection reforms affect the agreement's entire content and structure. Whether the parallel negotiating strands are compatible with one another is contested. To that extent it is crucial that TTIP and TiSA leave sufficient flexibility to permit as yet undefined future data protection rules to apply to the European Union's trade relations. Data protection experts therefore demand that TTIP make no decisions that hamper implementation of the GDPR. Any vagueness would open up possibilities for companies to take legal action if they believed that the EU arrangements contradicted international agreements. In the case of TTIP, the possibility of such cases being brought in the investor-state dispute settlement framework further inflames the critics' fears. Whether adequate flexibility to implement the EU data protection rules effectively can be ensured despite TTIP and TiSA will depend above all on the following factors:

- Because TTIP and TiSA are being negotiated after the GDPR was finalised, their

data privacy implications can still be reviewed.

- Whether the exceptions in GATS and those still to be defined in TTIP and TiSA are sufficiently strong and clearly formulated remains to be examined.
- Another significant question is the extent to which (trade) experts can correctly assess the technical and privacy-relevant consequences of liberalisation agreements for services that have yet to be developed. This question is especially relevant for decisions in the context of the negative list approach, where a sector as a whole is liberalised, with the exception of explicitly listed activities. Here there is a great risk that liberalisation will encompass highly data-relevant products that have yet to be developed, where the data protection consequences of liberalisation cannot yet be assessed.
- A clear definition of new digital services is important, along with clarification of whether they can be clearly assigned to one of the four WTO modes of supply (see above, p. 2).

In this situation it would be advisable for future free trade agreements to include clauses at least as strong as those in the agreement with South Korea, as these are clearer than the GATS exceptions.

All these factors suggest that actors in the fields of information and communication technology, data protection and trade negotiations should cooperate more closely.

The new EU trade strategy of October 2015, "Trade for All", offers starting points for the outstanding discussion about the relationship between trade and data protection. While businesses seek to maximise the free flow of data, they also depend on the security of their data (especially protection of intellectual property). The EU Network and Information Security Directive in December 2015 addresses the question of data security, instituting a duty to report significant cyberattacks and introducing minimum requirements for security of data associated with the protection of critical infrastructure. The equivalent law in the United States, the Cybersecurity Information Sharing Act (CISA), is less far-reaching. It permits US companies to pass data on unspecified IT threats to US authorities such as the Department of Homeland Security, which may in turn pass it to other institutions such as the FBI and the NSA. Critics object that it neglects data protection. Multinationals would prefer regulations on both sides of the Atlantic to be as similar as possible.

The overall current situation is one of legal insecurity for companies and consumers in the transatlantic economic space. Solutions are not immediately obvious. The IT industry is already preparing for stricter rules, applying pseudonymisation, encryption and other methods for anonymising personal and meta-data. US firms like Microsoft have responded directly to the Safe Harbour ruling, and plan to enable the customers of their cloud services to store and process their data in Germany at Deutsche Telekom computing centres. In this arrangement the Telekom subsidiary T-Systems will monitor and control international access to customer data. Microsoft and its agents will be able to access the data only with the consent of T-Systems or the customer. As this demonstrates, creating a server infrastructure within the European Union and legally and technically outsourcing access rights would be a viable option for other cloud services too. The EU-US Privacy Shield will not solve the problem of legal uncertainty for firms operating on both sides of the Atlantic, nor will it set rules for data transfer outside the transatlantic market. But does at least open the door for future legal integration.



**SWP**
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3–4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1861-1761

*Translation by Meredith Dale*

(English version of SWP-Aktuell 10/2016)