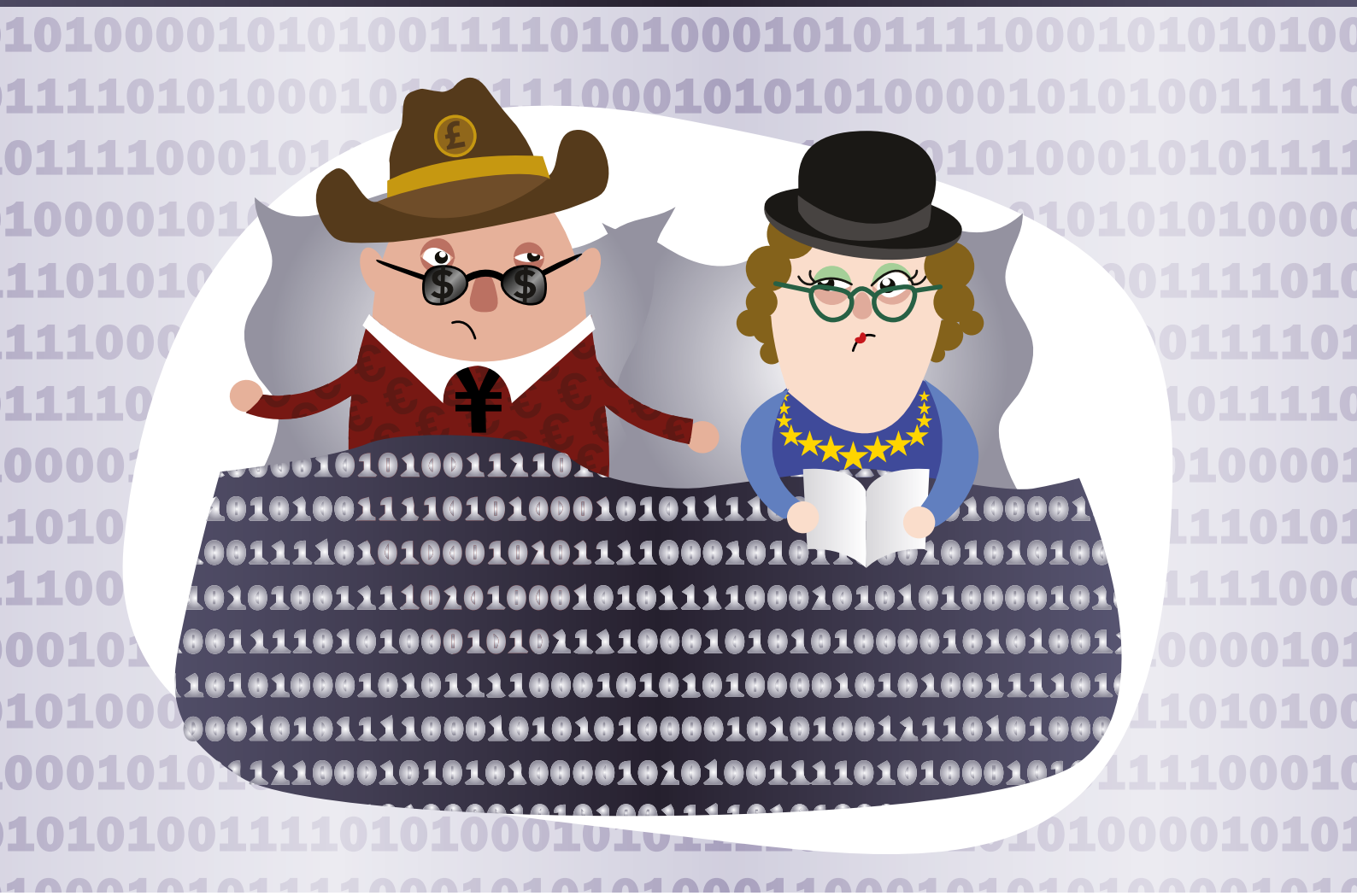
TRADE AND PRIVACY: COMPLICATED BEDFELLOWS?

How to achieve data protection-proof free trade agreements

Kristina Irion, Svetlana Yakovleva, and Marija Bartl



UNIVERSITY OF AMSTERDAM

IViR

Study commissioned by the European Consumer Organisation/Bureau Européen des Unions de Consommateurs (BEUC), Center for Digital Democracy (CDD), The Transatlantic Consumer Dialogue (TACD) and European Digital Rights (EDRi).

Disclaimer

The opinions expressed in this work reflect the authors' own views and do not necessarily reflect those of the commissioning organisations. The project has been carried out in full compliance with the European Code of Conduct for Research Integrity.

Authors

Kristina Irion	Senior Researcher, Institute for Information Law (IViR) at the University of Amsterdam (NL) and Associate Professor at the School of Public Policy (SPP), Central European University, Budapest (HU)
Svetlana Yakovleva	Project Researcher, Institute for Information Law (IViR) at the University of Amsterdam (NL)
Marija Bartl	Assistant Professor, Centre for the Study of European Contract Law (CSECL) at the University of Amsterdam (NL)

Suggested citation:
K. Irion, S. Yakovleva and M. Bartl, "Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements", independent study commissioned by BEUC et al., published 13 July 2016, Amsterdam, Institute for Information Law (IViR).

Layout (except cover page): Suzanne Bakkum

Amsterdam, 13 july 2016

Institute for Information Law (IViR)
Vendelstraat 7
1012 XX Amsterdam
The Netherlands
Website: http://ivir.nl/
Phone: + 31 (0)20 525 3406
Email: ivir@ivir.nl

Table of contents

Table of contents (details)

Abbreviations

BCRs	Binding Corporate Rules
CETA	(EU-Canada) Comprehensive Economic and Trade Agreement
CJEU	Court of Justice of the European Union
DPD	(EU) Data Protection Directive
DSS	(WTO) Dispute Settlement System
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EU	European Union
FRA	(EU) Agency for Fundamental Rights
GATS	(WTO) General Agreement on Trade in Services
GATT	(WTO) General Agreement on Tariffs and Trade
GDPR	(EU) General Data Protection Regulation
ICS	Investment Court System
ISDS	Investor-to-State Dispute Settlement
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TiSA	Trade in Services Agreement (negotiations)
TTIP	(EU-US) Transatlantic Trade and Investment Partnership (negotiations)
US	United States of America
WTO	World Trade Organization

Summary

This independent study assesses how EU standards on privacy and data protection are safeguarded from liberalisation by existing free trade agreements (the General Agreement of Trade in Services (GATS) and the Comprehensive Economic and Trade Agreement (CETA)) and those that are currently under negotiation (the Trans-atlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TiSA)). It was jointly commissioned by the European Consumer Organisation (BEUC), the Center for Digital Democracy (CDD), the Transatlantic Consumer Dialogue (TACD) and European Digital Rights (EDRi), and executed by the Institute for Information Law (IViR) at the University of Amsterdam.

Based on the premise that the EU does not negotiate its privacy and data protection standards, the study clarifies safeguards and risks in respectively the EU legal order and international trade law. In the context of the highly-charged discourse surrounding the new generation free trade agreements under negotiation, this study applies legal methods in order to derive nuanced conclusions about the preservation of the EU's right to regulate privacy and the protection of personal data.

The EU legal order itself carries robust safeguards that protect EU privacy and data protection standards from (involuntary) liberalisation via the international trade agreements to which the EU is party. Not only are the fundamental rights to privacy and the protection of personal data well entrenched in EU primary law, but the principle of "autonomy of the EU legal order" and the lack of "direct effect" in conjunction with international trade law moreover preclude EU law from being automatically changed.

International trade agreements to which the EU is or will become a party should be consistent with all aspects of EU legislation on data protection, which vests, by international standards, the highest level of protection. Even when it cannot overturn EU legislation, international trade law should not become a venue for challenging the EU approach to the protection of personal data. The EU's global policy model and its legitimacy vis-à-vis its trade partners must not be undermined.

The contemporary ubiquity of the processing of personal data in cross-border trade in services renders data protection measures especially susceptible to being probed for their compliance with the EU's commitments in international trade agreements. The potential for trade disputes is not just an issue of the EU entering into further commitments on data flows, but a current risk with existing commitments in core disciplines in international trade agreements.

The EU's right to regulate, as recognised in international trade agreements, is subject to certain trade-conforming limitations and conditions. Under the GATS, for example, a party may adopt measures that are not inconsistent with the obligations and commitments assumed under this agreement. In the case that measures are found to be GATS-inconsistent, the general exceptions are the central bulwark for defending a party's right to regulate, and the only context within which regulatory objectives and concerns can be deliberated.

As a concrete example, the EU rules on transfers of personal data to third countries (Chapter IV of the Data Protection Directive), which aim to protect the remainder of EU data protection law from circumvention, have been exposed to a finding of GATS inconsistency. This means that the requirements of the general exceptions must be met in order to defend this EU measure. Entering into additional commitments on free data flows without a prudential carve-out for a party's privacy and data protection laws would only raise the bar for justification, and compound pressure on the general exceptions.

The GATS carries an explicit exception on privacy that is subject to a series of tests, leaving a certain margin for interpretation that cannot be fully anticipated from a solely EU-centric perspective. There is an entire spectrum of opinions as to whether or not some measures of EU data protection law would meet the general exceptions. In addition, EU policy and practice could fall short of the required level of consistency, for example in how the Commission administers adequacy decisions.

Not only is there a need to update trade rules for the digital economy and cross-border data flows but, from an EU perspective, it is also necessary to upgrade the exception for privacy and data protection. Entrusting the EU's right to regulate in new generation free trade agreements to the general exceptions, which are modelled after the GATS, would perpetuate a residual legal risk. Note in this respect that EU negotiators injected an additional safeguard for EU rules on the transfer of personal data to third countries in CETA's Financial Services Chapter.

This study underscores the formula of the European Parliament that new free trade agreements should contain "a comprehensive, unambiguous, horizontal, self-standing and legally binding provision based on GATS Article XIV which fully exempts the existing and future EU legal framework for the protection of personal data from the scope of this agreement, without any conditions that it must be consistent with other parts of the [agreement]."

As long as this is not granted, the EU should not enter into additional commitments concerning free data flows in new and enhanced disciplines that lack any reference to the party's privacy and data protection laws. In relation to new provisions that each party shall adopt or maintain a privacy and data protection legal framework, they should not be linked to any qualitative conditions (e.g. "adequate", "non-discriminary"), nor to principles and guidelines of international bodies if these would introduce a ceiling for the acceptable level of protection.

The table below lists all of the safeguards and risks identified in the study. The recommendations that follow are addressed to EU decision makers and trade negotiators respectively, and list practical steps for how to strengthen and modify existing safeguards on privacy and data protection in order to make them fit for purpose in next generation free trade agreements.

Table 1: Overview summarising the findings on safeguards and risks

	EU law	International trade law
Safeguards	1. Charter rights to privacy and data protection ***(strong)*** 2. Independent supervision ***(medium)*** 3. Scope of application of EU data protection law ***(medium)*** 4. Requirement of third countries' adequate level of protection ***(strong)*** 5. Principle of autonomy of EU legal order ***(strong)*** 6. Absence of direct effect ***(strong)*** 7. Advisory opinion procedure provided for in Article 218(11) TFEU ***(strong)***	8. General exceptions modelled after GATS Article XIV(c)(ii) ***(medium)*** 9. New exceptions in Understanding in Commitments on Financial Services and CETA's Chapter on Financial Services ***(strong)*** 10. Stand-alone right to regulate ***(weak)*** 11. Investment protection limited to monetary compensation ***(medium)***
Risks	I. EU international relations emphasise international trade in services ***(medium)*** II. Commission's assessments and decisions on third countries' adequate level of protection ***(strong)*** III. Reliance on contractual safeguards and derogations in relation to transfer of personal data to third countries in relation to national security ***(strong)***	IV. Personal data processing is inextricably intertwined with the ordinary conduct of business in most sectors ***(strong)*** V. EU rules on the transfer of personal data to third countries trigger non-discrimination commitments ***(medium)*** VI. EU measures in relation to the transfer of personal data to third countries not meeting the requirements of "necessity to ensure compliance" and/or the *chapeau* of the general exceptions ***(strong)*** VII. Qualitative requirements and/or reference to international standards in relation to new positive obligations to ensure privacy and data protection ***(medium)*** VIII. New commitments on data flows without a prudential carve-out for a party's data protection law ***(strong)*** IX. Regulatory co-operation in relation to producing impact assessments and independent supervision ***(weak)***

Recommendations

The following recommendations are addressed respectively to EU decision makers and trade negotiators, and list practical steps for how to strengthen and modify existing safeguards on privacy and data protection in order to make them fit for purpose in next generation free trade agreements.

1. Underscoring the formula of the European Parliament that new free trade agreements better entrust their right to regulate in the field of privacy and data protection to

   > ... a comprehensive, unambiguous, horizontal, self-standing and legally binding provision based on GATS Article XIV which fully exempts the existing and future EU legal framework for the protection of personal data from the scope of this agreement, without any conditions that it must be consistent with other parts of the [agreement].[1]

2. Underscoring the European Parliament's position that additional commitments concerning free data flows in new and enhanced disciplines should not be disconnected from any reference to the party's privacy and data protection laws. CETA's Chapter on Financial Services, for example, introduces an exception for regulating the cross-border transfer of personal data.

3. In relation to new positive obligations that each party shall adopt or maintain a privacy and data protection legal framework, these should not be linked to any qualitative conditions (e.g. "necessary"), nor to the principles and guidelines of international bodies if these would introduce a ceiling for the acceptable level of protection.

4. Pursuant to the EU's current practice, insert "no direct effect" clauses in free trade agreements and Council decisions approving these free trade agreements. In order to forego any finding of "direct effect", avoid reference in EU legal acts to specific provisions in free trade agreements.

5. With a view to protecting EU privacy and data protection standards, it should be incumbent on the European Data Protection Supervisor (EDPS) to issue opinions on the texts of free trade agreements that the EU plans to adopt.

6. When there is reason to believe that a new free trade agreement to which the EU will become a party negatively affects EU privacy and data protection standards, a Member State, the European Parliament, the Council or the Commission should initiate an advisory opinion procedure at the Court of Justice as provided for in Article 218(11) of the TFEU.

7. Adequacy assessments and decisions by the Commission must not grant differential treatment to some third countries and not to others. The Commission should adopt procedural rules for the administration of the assessment of adequate levels of protection for third countries, thereby facilitating "consistency of enforcement".

1 Resolution of 3 February 2016 containing the European Parliament's recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA), (2015/2233(INI), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0041+0+DOC+XML+V0//EN> (accessed 10 May 2016), para. (c).iii.

8. The Commission should publish impact assessments on preserving the EU's right to regulate in areas of public interest and legal reasoning based on which it concludes, with sufficient certainty, that EU data protection law in all aspects satisfies the requirements of the general exceptions modelled after GATS Article XIV(c)(ii).

9. EU institutions should commission a study into enterprise customers' preferences in the outsourcing and provisioning of computer services involving the personal data processing in order to build an evidence base supporting the fact that EU data protection law is a differentiating factor in the competitive relationship between services and service suppliers.

I. Introduction

Without doubt, trade in services is greatly facilitated by information technologies and global flows of data. A recent study estimates that cross-border data flows now exert a larger impact on global GDP than does trade in goods.[2] Enabling global data flows, including individuals' personal data, has taken centre stage in international policy efforts, which are strongly backed by stakeholders from industry.[3]

Next to astounding estimates on the positive feedback loop of global data flows on international trade and welfare, the fact that such data often includes individuals' personal data can easily appear subordinated. Whereas it cannot be denied that divergent data protection standards affect cross-border trade in services, it is moreover plausible that such regulations are an important ingredient in buttressing consumer trust in electronic commerce and online transactions.[4]

The EU is not only a world leader in international trade[5] but is also a spearhead, by international standards, in the legal protection of privacy and personal data. The Charter of Fundamental Rights of the European Union guarantees, in its Articles 7 and 8, the fundamental rights of individuals to privacy and data protection respectively. EU data protection law regulates in detail the processing of personal data and the attendant safeguards and rights.

The EU is a party to the WTO agreement, including its General Agreement on Trade in Services (GATS). Furthermore the text of the Comprehensive Economic and Trade Agreement (CETA) with Canada has been finalised, and the EU is currently negotiating another agreement with the United States, the so-called Transatlantic Trade and Investment Partnership (TTIP). In addition, the EU is negotiating a plurilateral agreement to further liberalise trade in services in the framework of the Trade in Services Agreement (TiSA).

Going beyond the GATS, the CETA, TTIP and TiSA agreements are very comprehensive and cover cross-border trade in services, which inevitably involves the processing and transferring of personal data in connection with the conduct of a service supplier's business. New quests for unrestricted flows of data are high on the agendas of international trade law in the making, and the EU is a party to these negotiations.

These agreements could therefore have an impact on EU data protection law. The European Parliament maintains that data protection and the right to privacy are first and foremost fundamental rights, and not trade barriers.[6] Against this background, it is essential

---

2 McKinsey Global Institute, *Digital Globalisation: The New Era of Global Flows*, March 2016, p. 83, available at <http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx> (accessed 10 May 2016).

3 E.g. UNCTAD, *Data protection regulations and international data flows: Implications for trade and development*, New York/Geneva, 2016, available at <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf> (accessed 10 May 2016); World Economic Forum, *Rethinking Personal Data: Strengthening Trust*, 16 May 2012, available at <https://www.weforum.org/reports/rethinking-personal-data-strengthening-trust> (accessed 10 May 2016).

4 Commission, *Data Protection, Special Eurobarometer 431*, June 2015, available at <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf> (accessed 10 May 2016).

5 The EU28 surplus stood at almost €163 billion in 2014. See Eurostat, "EU surplus down to almost €163bn in 2014. The USA and EFTA countries, main trading partners," news release 5/2016, 12 January 2016, available at <http://ec.europa.eu/eurostat/documents/2995521/7130584/2-12012016-AP-EN.pdf/f79c2805-76e2-435e-9883-69606e0a2bcd> (accessed 20 April 2016).

6 European Parliament (fn 1); see also Alexander Dix, *Datenschutz und transatlantische Freihandleszone*, Karlsruher Dialog zum Informationsrecht, Band 5, p. 8f., available at <http://d-nb.info/1043752382/34> (accessed 10 May 2016).

to verify whether the necessary safeguards are solid enough to ensure that these fundamental rights, including the rights to privacy and data protection, are protected.

This study aims to assess how EU standards on privacy and data protection are safeguarded from liberalisation by existing free trade agreements (the GATS and CETA), as well as by those currently under negotiation (TiSA and TTIP). A further objective is to formulate recommendations for the strengthening or modification of current safeguards in order to ensure that EU data protection rules will be respected by trade partners.

As a point of departure, the study looks separately at legal risks and safeguards in EU law and international trade law. The legal assessment of EU privacy and data protection standards in international trade law takes as a starting point the interpretation and application of the GATS in a hypothetical trade dispute. Against this background, a comparative analysis with next generation international trade agreements can offer a number of clues about the substantive changes and their likely effects.

The legal argument revolves around the EU's regime for the transfer of personal data to third countries, which are sorted into different categories depending on whether or not they ensure adequate levels of protection. Additionally, where they fall inside the scope of application, services and services suppliers would have to adhere to EU data protection law in the cross-border supply of services.

This study employed mixed methods including literature review, desk research and applied law in line with the European legal method. Data included official and unofficial documentation on the international trade agreements in the scope of this study, and text mining for keywords. The texts of the GATS and CETA agreements, as well as the currently available draft texts of TTIP and TiSA, are annexed in a structured overview to facilitate comparison.

As part of the study, the authors conducted interviews with three trade negotiators at the European Commission. The interviews were held at the European Commission offices in Brussels on Monday 14 March 2016.

The study identified and ranked risks and safeguards according to their relative impact (weak, medium or strong) using a risk assessment approach.

The rest of the study is structured as follows: Chapter II covers the entrenchment in EU law of the rights to privacy and the protection of personal data, and introduces the institutions that contribute to the protection of these laws. This Chapter also explains how international trade agreements are adopted by the EU and incorporated into its legal system. Chapter III introduces the international trade agreements covered in this study: the GATS, its potential successor the TiSA, CETA and TTIP. In Chapter IV, the GATS is applied to EU data protection law and implementation measures. This lays the groundwork for the subsequent comparative analysis in Chapter V, which includes newer free trade agreements in the making. The Conclusion includes a summary of the findings, as well as recommendations for protecting EU privacy and data protection standards against liberalisation via free trade agreements.

The authors carried out this study independently, and in full compliance with the European Code of Conduct for Research Integrity.[7]

7 European Science Foundation, "The European Code of Conduct for Research Integrity", March 2011, available at <http://www.esf.org/fileadmin/Public_documents/Publications/Code_Conduct_ResearchIntegrity.pdf> (accessed 1 February 2016). We are grateful to Professor Stephan Schill, Professor Ingo Venzke, Professor Nico van Eijk, and Dr. Szilard Gaspar-Szilagyi, all from the University of Amsterdam, for their valuable comments.

II. European union law

This section covers EU law and serves four purposes. First, it conveys how the rights to privacy and data protection are guaranteed and protected in EU law. In a second step, it explains how EU secondary law comes to terms with the flow of personal data to third countries. Third, it introduces the institutions that protect individuals' rights to privacy and data protection at the EU and Member State levels. Finally, it explains the EU's common commercial policy, and how international trade law is incorporated into the EU legal order.

1. The rights to the protection of privacy and personal data

After a quick review of the right to privacy in international human rights law, this section covers the evolution of the protection of the right to privacy, and the coming into existence of a separate fundamental right to the protection of personal data in EU law.

a. Human rights and legislation in Europe

International human rights law recognises the individual's right to privacy, notably in Article 12 of the Universal Declaration of Human Rights and in Article 17 of the International Covenant on Civil and Political Rights. In Europe, the right to privacy is guaranteed under Article 8 of the European Convention on Human Rights (ECHR), and forms part of the constitutional tradition of European countries.

The right to privacy traditionally protects an individual's private and family life, home and correspondence against arbitrary or unlawful interference by government. The ECHR, seated in Strasbourg, has ruled that its Member States have a positive obligation to give effect to the right to privacy under Article 8 of the ECHR.[8] This means that countries must issue legislation to ensure that this fundamental right is observed with respect to private sector activities.

The notion of a right to the protection of personal data evolved in response to advancements in automated data processing capabilities. In 1981, the Council of Europe adopted Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. The ECHR interpreted the protection of personal data as falling within the broad scope of the right to respect for privacy in Article 8 of the ECHR.[9] Throughout the 1990s, data protection legislation developed rapidly in European countries.

b. EU law and the Charter of Fundamental Rights of the European Union

In 1995, the EU adopted the Data Protection Directive (DPD) which is the first comprehensive data protection framework aiming to protect the fundamental right to privacy with respect to the processing of personal data.[10] EU Member States then issued legislation pursuant to this Directive incorporating the defining conceptual approach of EU data protection law.

The 2000 Charter of Fundamental Rights of the European Union introduced, in addition to the right to respect for privacy (Article 7), the right to the protection of personal data (Article 8). With the entry into force of the Lisbon Treaty in 2009, the Charter was accorded binding legal effect (Article 6(1) of the Treaty on European Union (TEU)). As a result, the right to data protection is now elevated to the status of a fundamental right in EU law:

8 ECtHR, *Marckx v Belgium* [1979], ECtHR 6833/74, para. 31, in relation to the right to respect for family life.
9 ECtHR, *Leander v Sweden* [1987], ECtHR 9248/81, para. 48.
10 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "Data Protection Directive", DPD), [1995], Official Journal L 281/31.

Article 8
Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Safeguard 1
Charter rights to privacy and data protection *(strong)*
The Charter is incorporated in EU primary law and hierarchically above incorporated international trade law.

For a fundamental right, the level of detail specified in Article 8 of the Charter is remarkable. Several core mechanisms of secondary EU data protection law found their way into the Charter, such as the principles relating to data quality, the need for a legitimate basis for the processing of personal data, and individuals' right to access and rectification. Ultimately, the right of individuals to control by an independent authority can potentially be very relevant in the context of the international transfer of personal data.

c. EU secondary law on the protection of personal data

In EU secondary law, the processing of personal data is regulated, thereby also giving effect to the fundamental rights to privacy and data protection in the private sector. For the purpose of this study, two EU legal instruments are relevant: the aforementioned DPD (95/46/EC) and the e-Privacy Directive (2002/58/EC).[11] The DPD lays down a general regulatory framework for the processing of personal data, which the e-Privacy Directive complements and elaborates upon for the electronic communications sector.

Based on the EU competence to establish an internal market though the approximation of Members States' national laws, these Directives are binding upon EU Member States (Articles 114(1) and 288 of the Treaty on the Functioning of the European Union (TFEU)). This means that EU Member States have adopted national laws to implement both the DPD and the e-Privacy Directive. This study, however, focuses solely on relevant EU law and does therefore not consider the law as applied at the EU Member State level.

The DPD has as its dual objectives the protection of the individual's fundamental right to privacy with respect to the processing of personal data, and the provision of a free flow of personal data between the Member States (Article 1). The Directive applies to the processing of personal data, whether this is entirely or partially automated or part of a filing system. As a horizontal instrument, the Directive covers personal data processing in the public and private sectors except when this falls outside the scope of community law or is exempt as a purely private or household activity (Article 3).

The definitions, principles on data quality, and legitimate grounds for the processing of personal data contained in the DPD (Articles 2, 6 and 7) are key to an understanding of the EU's regulatory approach. Taken together, they circumscribe a strict legal framework for the lawful handling of personal data. Independent authorities in the Member States supervise compliance within this legal framework. What matters for this study is that the legal framework can also apply to non-EU actors, and that the transfer of personal data to third countries is also regulated (see Section II.2).

The e-Privacy Directive, as a sector-specific instrument, is primarily addressed to providers of public electronic communications services and networks. It contains requirements for the processing of traffic and location data, among others. Nonetheless, certain provisions of the e-Privacy Directive are of general application, namely rules on unsolicited commercial commu-

11 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the "e-Privacy Directive"), [2002], Official Journal L 201/37.

nications, and storage of and access to information already stored in the terminal equipment of a subscriber or user (the so-called "cookie rule").

d. EU data protection reform

Another development of the Lisbon treaty is that the EU legislator has the exclusive competence to legislate in the area of data protection (Article 16(2) TFEU). In 2016, the EU legislator adopted the General Data Protection Regulation (GDPR, (EU) 2016/679),[12] which will – once it enters into force on 25 May 2018 – replace the DPD. As a regulation, the GDPR will be binding in its entirety and directly applicable throughout the EU (Article 288 TFEU). While this study is based on the currently applicable DPD, relevant changes as a consequence of the imminent GDPR are flagged.

The GDPR is the outcome of a four-year long reform of EU data protection law that pursued two general objectives: to overcome the persistent fragmentation of the internal market due to divergent national implementations of the DPD in the Member States, and to modernise data protection law and enhance its effectiveness in the protection of individuals' fundamental rights. Although the regulation by and large preserves the regulatory approach of its predecessor, it includes many clarifications, adjustments and regulatory innovations.

Now that the GDPR has been adopted, the European Commission is preparing the reform of the e-Privacy Directive. A legislative proposal is expected for mid-2017.

2. EU legal approach to cross-border flows of personal data

This section offers essential background for understanding how the Directive and its successor, the GDPR, come to terms with the processing of personal data in the commercial sector and with cross-border flows of personal data.

a. Under the Data Protection Directive (DPD)

Since its inception in 1995, the DPD has recognised that personal data moves across borders between as well as beyond EU Member States. After all, the Directive was conceived as an instrument to remove obstacles to the flow of personal data in the internal market. Furthermore, the transfer of personal data to third countries has been subject to additional safeguards from the outset. The DPD's scope of application already includes cross-border flows of personal data to a certain extent, in addition to the specific rules in Chapter IV on transfer of personal data to third countries.

i. Scope of application

A legal act's scope of application has material, personal and territorial dimensions, which together determine when it can be applied. The DPD's scope of application is in all respects broadly defined and interpreted. As a result, it already covers the processing activities of personal data to some extent, even if actors are not established inside the EU.

The DPD applies to instances of the automated processing of personal data. Hence, the definitions of "personal data" and "processing" circumscribe the material scope of the Directive. "Personal data" is defined broadly, and covers any information relating to an identified or identifiable natural person (Article 2(a)). A person is deemed identifiable if s/he can be directly or indirectly identified, even by reference to an identification number (Ibid). Data not relating to an individual (anonymous data), or data that has been "rendered

12 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the "General Data Protection Regulation", GDPR), [2016], Official Journal L 119/1.

anonymous in such a way that the data subject is no longer identifiable", is not considered personal data.[13]

Additionally, the term "processing" is broadly defined to mean any operation that is performed upon personal data, with a range of examples including the collection, use or disclosure of personal data (Article 2(b) DPD). The CJEU ruled in the *Bodil Lindqvist* case to include the operation of loading personal data on an internet page in the definition.[14]

Furthermore, the (online) collection of personal data from individuals constitutes a processing operation in the meaning of the Directive. And although the DPD does not define the term "transfer", the CJEU ruled in the case *Schrems v Data Protection Commissioner* that the (spatial) transfer of personal data from an EU Member State to a third country qualifies as processing.[15]

The personal scope of application rests on the definitions of "controller" and "processor", both of whom are subject to compliance with the DPD. "Controller" is defined as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (Article 2(d) DPD).

A "processor" is an auxiliary who processes personal data on behalf of the controller (Article 2(e) DPD). All technical means, such as the software and equipment used for the processing of personal data, are attributed to the actor operating them, who is – depending on the circumstances – either the controller or the processor.

Article 4 of the DPD prescribes the territorial scope and, hence, when EU law applies. This is when the processing is carried out in the context of the activities of an establishment of the controller on the territory of a Member State (Article 4(1)(a) DPD). This should be read in conjunction with Recital 19, following which the "establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements" and that "the legal form of such an establishment, whether simply [a] branch or a subsidiary with a legal personality, is not the determining factor". Thus, even if the controller is not established on EU territory, but for purposes of processing personal data makes use of equipment situated on the territory of a Member State, the DPD applies (Article 4(1)(c)). It is therefore evident that depending on the circumstances, foreign controllers can also be subject to EU data protection law.

The CJEU recently issued an expansive interpretation of the territorial scope of the DPD in relation to a company with global operations.[16] In the *Google Spain v AEPD* case, the court held that personal data processed abroad is nevertheless carried out in the context of an EU establishment if the activities of the establishment are inextricably linked to the processing of personal data by a foreign controller.[17] In a nutshell, the court connected the dots between Google's free search service, for which the personal data of EU individuals is processed, and the company's revenue-making online advertisement arm, which is facilitated via a local establishment. In the light of the ruling, it is thus not necessary that the establishment itself processes personal data in order for the DPD to be applied.

13 Article 29 Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007, p. 21, available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> (accessed 20 April 2016).

14 CJEU, case C-101/01 (*Bodil Lindqvist*), judgment of 6 November 2003, ECLI:EU:C:2003:596, para. 23.

15 CJEU, case C-362/14 (*Maximillian Schrems v Data Protection Commissioner*), judgment of 6 October 2015, ECLI:EU:C:2015:650, para. 45.

16 CJEU, case C-131/12 (*Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*), judgment of 13 May 2014, ECLI:EU:C:2014:317.

17 Ibid., para. 60.

Following an opinion issued by the Article 29 Working Party, Article 4(1)(c) of the DPD is especially relevant in the light of new technologies and the internet, which together facilitate the collection and processing of personal data at a distance, irrespective of the controller's physical presence in EU territory.[18] The use of equipment located in the EU can be interpreted to include any means used by a controller with the intention to process personal data. Subject to a case-by-case assessment, examples could include questionnaires used to collect personal data, or software installed on personal devices through which personal data is collected and sent to a controller in a third country.

ii. Transfer of personal data to third countries

EU data protection law establishes an internal market for the flow of personal data and prescribes limitations on the transfer of personal data to third countries. Navigating the ensuing landscape is a bit more complex than solely differentiating between EU Member States and third countries. First of all, the 28 EU Member States, together with Iceland, Liechtenstein and Norway, form the European Economic Area (EEA), an enlarged internal market in which the DPD applies. Hence, the internal market for personal data flows is comprised of the EU/EEA countries.

Chapter IV of the DPD sets out the rules for the transfer of personal data originating in the EU to third countries. The Directive recognises that cross-border flows of personal data are necessary to the expansion of international trade, under the premise that such transfers may take place only if the third country ensures an adequate level of protection (Recital 56, Article 25(1)). The CJEU summarises the rationale for these rules as an anti-circumvention mechanism:

> Furthermore, the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries.[19]

Henceforth, the Directive provides for a principle differentiation between third countries that ensure an adequate level of protection (Article 25), and third countries without an adequate level of protection (Article 26). Third countries, however, do not automatically fall into either category. The junction to finding an adequate level of protection involves an assessment that concludes with a decision that a third country does (or does not) satisfy the requirements. In principle, transfers of personal data to third countries not ensuring an adequate level of protection must be prohibited (Recital 57) unless one of the derogations in Article 26 of the Directive applies.

Safeguard 4
Requirement of third countries' adequate level of protection *(strong)*
This requirement protects EU data protection law against circumvention and is met when third countries' protection of personal data is essentially equivalent to EU standards.

This leads to the question of what an "adequate level of protection" means, and how that is to be assessed. In the absence of a legal definition, the meaning ascribed to it by the CJEU is that a third country's legal order must afford a level of protection "that is essentially equivalent to that guaranteed within the [EU] by virtue of Directive 95/46 read in the light of the Charter."[20] The Directive holds an extensive list of criteria that must be taken into account:

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed

18 Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, adopted on 16 December 2010, WP 179, p. 18, available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf> (accessed 20 April 2016).

19 CJEU, (*Schrems v Data Protection Commissioner*), (fn. 17), para. 73.

20 Ibid.

> processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country (Article 25(2)).

Decisions on a third country's adequate level of protection are issued by the European Commission or, as long as this has not happened, by Member States' national supervisory authorities (Article 25(6) DPD).[21] To date, the Commission has issued decisions attesting to an adequate level of protection in eleven countries. Hence, personal data originating from the EU/EEA can also be transferred to Andorra, Argentina, Canada, the Faeroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. The Commission has thus far never adopted a decision that found that a third country does not ensure an adequate level of protection.

As a different route to an adequacy finding, the EU and the US concluded the so-called "Safe Harbour" agreement. This was formally adopted in 2000 by a Commission adequacy decision (2000/520) incorporating the agreement. In 2015, the CJEU invalidated this decision for the reason that the Commission's decision did not include a statement that the US indeed ensures an adequate level of protection by reason of its domestic law or its international commitments.[22] Recently, the EU and the US have been negotiating a new scheme for transatlantic personal data flow, the so-called "Privacy Shield". In order to confer legal effect to the "Privacy Shield", the Commission must still endorse it with an adequacy decision.

Article 26 of the DPD provides for a number of derogations from the principle that the transfer of personal data to third countries may take place only if the third country ensures an adequate level of protection. These derogations are expressly intended for third countries that do not ensure an adequate level of protection, including those that have not been formally granted an adequacy decision. Such derogations can include the use of standard contractual clauses, ad hoc measures, or reliance on the conditions provided for in Article 26(1) of the DPD.

Ad hoc measures incorporate contractual safeguards, namely standard contractual clauses pre-approved by the Commission (Article 26(4) DPD) or authorisations of personal data transfers with appropriate contractual clauses (Article 26(2) DPD). The latter is also the legal basis for the approval of Binding Corporate Rules (BCR) by the national supervisory authorities.[23]

Additionally, Article 26(1) of the DPD contains a menu of conditions upon which a transfer of personal data to a third country that does not ensure an adequate level of protection can be based. With a view to international commerce, the individual's unambiguous consent to the transfer and the performance of a contract are especially relevant derogations, among others. As a result, cross-border transfers to third countries that are deemed not to afford an adequate level of protection remain possible, albeit subject to stricter rules assessed on a case-by-case basis.

iii. EU rules on transfer following the CJEU ruling invalidating the EU-US Safe Harbour agreement

The Court's 2015 ruling in the case *Maximillian Schrems v Data Protection Commissioner* is highly relevant to the subject of this study, as its factual background specifically concerns

21 Ibid., para. 50.

22 Ibid., para. 97.

23 As provided for by the procedures and rules laid down by the Article 29 Working Party, see <http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm> (accessed 20 April 2016).

the transfer by a private company of personal data originating from EU individuals to the US. In a nutshell, the Court interprets the Commission's obligation when rendering an adequacy decision under Article 25(6) DPD that:

> [...] it must find, duly stating reasons, that a third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order...[24]

It is important to note that the justices did not examine the content of the safe harbour principles, but could still invalidate the Commission's adequacy decision because it did not satisfy the requirements for concluding that a third country ensures an adequate level of protection.

The Court nevertheless argued that interference with the rights to privacy and the protection of personal data must be limited to what is strictly necessary, and that the right to effective judicial protection must be observed. The Court considered that:

> [L]egislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the [EU] to the [US] without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail.[25]

> […] legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.[26]

> […] legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.[27]

The CJEU's reasoning is directly based on Articles 7 and 8 of the Charter, and hence superior to secondary law. This has given rise to questions about the compatibility of the DPD rules for transfers of personal data to a third country that does not ensure an adequate level of protection with the Charter. The reason is that derogations provided for in Article 26 of the DPD are not capable of preventing preemptive blanket surveillance by a third country:

> None of the provisions of the European instruments designed to frame international data transfers between private parties provide a legal basis for the transfer of data to a third country authority for the purpose of massive and indiscriminate surveillance (whether Safe Harbor, binding corporate rules or standard contractual clauses).[28]

---

24 CJEU, (*Schrems v Data Protection Commissioner*), (fn. 17), para. 96.

25 Ibid., para. 93.

26 Ibid., para. 94.

27 Ibid., para. 95.

28 Article 29 Working Party, Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party, adopted on 26 November 2014, para. 10, available at <http://ec.europa.eu/justice/data-protection/Article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf> (accessed 10 May 2016).

Ultimately, only the CJEU can review the legality of EU legislation, and only the CJEU has the jurisdiction to invalidate these acts. For the time being, the DPD continues to provide a legal basis for transfers of personal data to third countries that do not ensure an adequate level of protection.

b. Under the General Data Protection Regulation (GDPR)

The forthcoming GDPR will bring some important clarifications on the scope of application of EU data protection law and in regard to personal data transfers to third countries.

i. New scope of application

The GDPR clarifies the material scope of application and takes a broader territorial scope. The definition of "personal data" clarifies that online identifiers and location data are covered (Article 4(1) GDPR). The territorial scope codified in Article 3 of the GDPR is modified to apply on the one hand to controllers established in the EU and, on the other hand, to controllers and processors not established in the EU.

Safeguard 3
Scope of application of EU data protection law *(medium)*
EU data protection law applies to most instances of cross-border supply of services to EU individuals.

The GDPR will apply to processing activities involving personal data connected to goods or services offered to individuals in the EU, or the monitoring of such individuals' behaviour within the EU (Article 3(2) GDPR). By linking the territorial scope to individuals' personal data originating in the EU instead of connecting it to the establishment of the controller or the location of equipment, the application of EU data protection law will expand vastly. The rationale behind the new territorial scope is to ensure that natural persons in the EU are not deprived of protection under EU data protection law (Recital 23 GDPR).

The GDPR's new territorial scope will come to the same conclusions as the CJEU's interpretation of the territorial scope of the DPD in the *Google Spain v AEPD* case, but its reach is much further. These new features will result in the application of EU data protection law to controllers and processors anywhere, insofar as they process EU-originating personal data in the course of commercial activities, and even if goods and services are offered free of charge. Furthermore, the GDPR protects individuals in relation to the monitoring of their behaviour within the EU.

ii. Revised rules on transfer of personal data to third countries

The GDPR will largely continue the legal approach to the transfer of personal data to third countries, subject however to a few new elements. Under the GDPR, there are now three main avenues for the transfer of personal data to third countries. The legal regime more appropriately distinguishes between transfers on the basis of an adequacy decision (Article 45 GDPR) and transfers subject to appropriate safeguards (Article 46 GDPR). In addition, and subsidiary to these two, there are derogations for specific situations in Article 49 of the GDPR.

The regulation clarifies that adequacy decisions by the Commission may concern specified sectors and even a territory within a third country. The assessment of the adequacy of the level of protection must take account of the elements listed in Article 45(2) of the GDPR. These include, among others, a review of the third country's legal system, in particular with regards to:

- public security, defence, national security and criminal law and the access of public authorities to personal data" (Article 45(2)(a) GDPR);
- effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred (Article 45(2)(a) GDPR); and
- the existence and effective functioning of one or more independent supervisory authorities in the third country. (Article 45(2)(b) GDPR).

In the event that the adequacy decision is no longer justified, the Commission can repeal, amend or suspend it with no retroactive effect. In the case of urgency, the Commission shall act expeditiously.

In the absence of an adequacy decision, personal data transfers to third countries potentially remain subject to appropriate safeguards, on the condition that enforceable data subject rights and effective legal remedies for data subjects are available (Article 46(1) GDPR). If they meet the requirements and are approved by the competent authorities at the EU and/or Member State level, codes of conducts, certifications and binding corporate rules are capable of providing for the lawful transfer of personal data to third countries (Article 46(2) GDPR). This is in addition to approved standard contractual clauses.

Article 49 of the GDPR provides for a menu of conditions, similar to that in the DPD, upon which a transfer of personal data to a third country can be based. However, it is clarified that these derogations for specific situations are subsidiary to transfers based on adequacy decisions or appropriate safeguards, and that further limitations may apply. In the absence of an adequacy decision, EU or Member State law may, "for important reasons of public interest, set limits to the transfer of specific categories of personal data to a third country..." (Article 49(5) GDPR).

An important new development in the GDPR tackles the exercise of third countries' disclosure authorities in relation to personal data protected by EU law. Article 48 of the GDPR does not authorise controllers and processors to disclose or transfer personal data to a third country based on the third country's authority. The exception is when this complies with international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the EU or a Member State.

The transitional clause in Article 96 of the GDPR provides that international agreements concluded by Member States, complying with EU law and involving the transfer of personal data to third countries, shall remain in force until amended, replaced or revoked.

3. Institutions at EU and Member State level

Aside from the legal protection afforded under the Charter and secondary regulation, institutions are important in implementing, supervising and defending the rights of individuals to privacy and data protection. The following section briefly introduces these institutions at EU and Member State level in relation to their role and specific contribution.

a. The Court of Justice of the European Union

The Court of Justice of the European Union (CJEU), seated in Luxembourg, interprets and reviews EU law (Article 19(1) TEU) and has sole jurisdiction in the invalidation of EU legal acts (Article 263 TFEU). Since the entry into force of the Charter, the CJEU has adopted a stronger interpretation of the DPD's normative function for the protection of individuals' fundamental rights:

> It is apparent from Article 1 of Directive 95/46 and recitals 2 and 10 in its preamble that that directive seeks to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms.[29]

29 CJEU, (*Schrems v Data Protection Commissioner*), (fn. 17), para. 39.

In two recent rulings, the CJEU performed a human rights-based review and invalidated EU acts for their noncompliance with the Charter.[30]

Under the advisory opinion procedure provided for in Article 218(11) of the TFEU, the CJEU can be called on to decide upon the compatibility of international agreements with EU law.

b. The European Commission

The European Commission (Commission) is the executive of the EU. The College of Commissioners heads the Commission and is composed of all 28 Commissioners (one from each EU Member State). The College strives to adopt all decisions by consensus, but can also act with a qualified majority.

The Commission has an internal structure that allocates the rights to privacy and data protection as well as international trade to different branches. The Directorate-General for Justice and Consumers holds the fundamental rights and data protection portfolio. It was in charge of the legislative proposals leading to the GDPR, and administers and prepares decisions on the adequate level of protection in third countries. Furthermore, it is the secretariat for the Article 29 Working Party.

The Directorate-General for Communications Networks, Content & Technology (DG CONNECT) has the lead on the reform of the e-Privacy Directive. The Directorate-General Trade is in charge of the EU's common commercial policy and hence conducts trade negotiations with third countries.

c. The European Data Protection Supervisor

The European Data Protection Supervisor (EDPS) acts as the independent supervisory authority of the EU within the meaning of Article 8(3) of the Charter. The general mission of the EDPS is to ensure that the fundamental rights and freedoms of individuals – in particular their rights to the protection of privacy and personal data – are respected when EU institutions and bodies process personal data or develop new policies.[31]

The EDPS issues opinions on EU legislative proposals, can intervene in actions brought before the CJEU, and collaborates with the Article 29 Working Party and the data protection authorities of the Member States. The EDPS has issued several opinions that informed this study, for example on safe harbour, covering inter alia TTIP negotiations,[32] on the legislative proposal for the GDPR, and on EU deliberations on privacy, data protection and trade in services.[33] There appears to be no consistent practice for issuing opinions on free trade agreements bearing on individuals' fundamental rights to privacy and data protection before their adoption by the EU legislator.

---

30 CJEU, joined cases C-293/12 and C-594/12 (*Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Others*), judgement of 8 April 2014, [2014], E.C.R. I-238; (*Schrems v Data Protection Commissioner*), ibid.

31 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, [2001], Official Journal L-8/1, Art. 41.

32 EDPS, Opinion on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU", 20 February 2014, available at <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-02-20_EU_US_rebuliding_trust_EN.pdf> (accessed 10 May 2016).

33 EDPS (Giovanni Buttarelli), "Trade agreements and data flows", Joint hearing of the INTA and LIBE committees, European Parliament, Brussels, 16 June 2015, available at <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-06-16_INTA_LIBE_EN.pdf> (accessed 10 May 2016).

d. The EU Fundamental Rights Agency

The EU Fundamental Rights Agency (FRA), based in Vienna, is primarily tasked with research and assists EU institutions in an advisory capacity. The FRA has published a range of reports and studies on the subject of individuals' fundamental rights to privacy and data protection. However, there is no report tackling the issue of cross-border transfer of personal data of EU individuals to third countries, or on the impact of free trade agreements on the fundamental rights to privacy and data protection.

e. The Article 29 Working Party

The Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up by Article 29 of the DPD (Article 29 Working Party) is an independent advisory body through which data protection authorities in the Member States, the EDPS and the Commission co-operate. The Article 29 Working Party issues opinions and recommendations that aim to streamline the interpretation of EU data protection law: on the level of protection in third countries, on codes of conducts, and on other ad hoc measures for transfers of personal data to third countries. It also pulls its weight in EU legislative procedures.

Notably, the Article 29 Working Party has bundled the competences of Member States' data protection authorities to adopt decisions on personal data transfers under Articles 25 and 26 of the DPD and, for example, introduced a co-ordinated procedure for approving Binding Corporate Rules (BCR) as a means of transferring personal data within a group of undertakings. Recently, the Working Party issued a negative opinion on the adequate level of protection afforded by the EU-US Privacy Shield, and has asked the Commission for further clarifications.[34]

With the entry into force of the GDPR, the European Data Protection Board will succeed the Article 29 Working Party.

f. Data protection authorities in the Member States

Data protection authorities in the Member States are institutions for which the establishment and independence is guaranteed under Article 8(3) of the Charter ("Compliance with these rules shall be subject to control by an independent authority.") The DPD, in Article 28(1), requires Member States to designate one or more public authorities to be responsible for implementing and enforcing national data protection laws pursuant to the Directive: "These authorities shall act with complete independence…".[35]

Member States are, however, free to organise their system of independent supervision within a single authority or – in federal states – several authorities. The case law of the CJEU affords the highest protection to the national data protection authority's independence (also in comparison with other sectors where EU law mandates the set up of independent regulatory authorities).[36]

These authorities can hear individual complaints and engage in legal proceedings, and they have investigative powers and effective powers of intervention including the power to temporarily or definitively ban the processing of personal data (Article 28(3) DPD). Data protection authorities can also suspend the transfer of personal data to third countries that do not ensure an adequate level of protection (25(4) DPD).

Safeguard 2
Independent supervision *(medium)*
Independent supervision protects against undue influence and also in the case of cross-border data transfers.

34 Article 29 Working Party, Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision, adopted on 13 April 2016, available at <http://ec.europa.eu/justice/data-protection/Article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> (accessed 10 May 2016).

35 Art. 28(1) DPD.

36 CJEU, case C-518/07 (*Commission v Germany*), judgement of 9 March 2010, [2010] I-01885; CJEU, case C-614/10 (*Commission v Republic of Austria*), judgement of 16 October 2012, ECLI:EU:C:2012:631; case C-288/12 (*Commission v Hungary*), judgement of 8 April 2014, ECLI:EU:C:2014:237.

4. International trade law in the EU legal order

This section explains how the international trade agreements entered into by the EU are adopted and incorporated into the EU legal system. Since the Lisbon Treaty took effect in 2009, the EU holds the exclusive competence for the common commercial policy. It should be recalled that the EU has legal personality (Article 47 TEU), which gives it the authority to conclude international treaties and to be a party to international conventions.

a. EU competence for the common commercial policy

Following the Lisbon treaty, the EU has exclusive external competence for the common commercial policy, including all aspects of trade in services, commercial aspects of intellectual property, and foreign direct investment (Articles 3(1)(e) and 207 TFEU). The acts of the EU must relate specifically to international trade in the sense that they should intend to "promote, facilitate or govern trade" and have "direct and immediate effects on trade".[37]

In this context, international trade agreements cover bilateral and multilateral agreements setting international trade and investment law. Although foreign direct investment is explicitly mentioned within the scope of the common commercial policy, it is still disputed whether portfolio investment and investors protection would fall under the scope of the EU exclusive competence.[38]

When areas covered by an international agreement do not fall within the exclusive competence of the EU or its Member States, or when such areas fall under the shared competence of the EU and its Member States, the agreement has to be concluded by both the EU and its Member States ("mixed agreements").

Together, the protection of personal data and the common commercial policy are the exclusive competence of the EU (Articles 16(2), 3(1)(e) and 207 TFEU).

b. Negotiation and adoption of international trade agreements

International agreements in the area of the common commercial policy are negotiated by the Commission based on the negotiating directives (mandate) adopted by the Council (Article 207(2) TFEU). The Commission reports to a special committee appointed by the Council and the European Parliament about the progress of the negotiations.

The decision to conclude the agreement is adopted by the Council after obtaining consent from the European Parliament (Article 218 (6)(a)(v) TFEU). This decision must be taken by qualified majority or, in special sensitive areas such as trade in culture, social or health services, through a unanimous Council vote (Article 207(4) TFEU).

Risk I
EU international relations emphasise international trade in services *(medium)*
EU institutions' approach is not fully aligned, with the CJEU being the guardian of EU law.

The founding treaties explicitly pronounce the values, principles and objectives that the EU shall pursue in its international relations, including when negotiating and entering into international trade agreements. In particular, the EU shall be guided by the universality and indivisibility of human rights and fundamental freedoms and their protection, as well as respect for human dignity and for the principles of the United Nations and international law (Articles 3(5) and 21 TEU).

c. The Court of Justice of the European Union's advisory opinion procedure

The CJEU can be called on in the advisory opinion procedure provided for in Article 218(11) of the TFEU. "A Member State, the European Parliament, the Council or the

37 CJEU, case C137/12 (*European Commission v. Council*), judgement of 22 October 2013, ECLI:EU:C:2013:675, para. 57.

38 See for example German Federal Constitutional Court, case 2 BvE 2/08 (*Lisbon*), judgement of 30 June 2009, ECLI:DE:BVerfG:2009:es20090630.2bve000208, paras. 1-421.

Commission may obtain the opinion of the [CJEU] as to whether an agreement envisaged is compatible with the Treaties" (Article 218(11) TFEU). In the event that the court's opinion is adverse, the agreement "may not enter into force unless it is amended or the Treaties are revised" (Ibid).

In relation to international agreements that provide for the transfer of personal data to third countries, the European Parliament actively uses the advisory opinion procedure.[39] In addition, there is an action for annulment that enables the Court to review the legality of acts adopted by EU institutions (Article 263 TFEU). This procedure has also been used to annul international agreements involving the transfer of personal data to third countries.[40] This advisory opinion procedure has the comparative advantage that the international agreement has not yet entered into force, and should thus be prioritised.

Safeguard 7
Advisory opinion procedure provided for in Article 218(11) TFEU *(strong)*
The CJEU can be called on to check a free trade agreement's compliance with EU law prior to its adoption.

d. How EU law incorporates international trade law

International agreements concluded by the EU – even if they are "mixed agreements" – are binding on EU institutions and Member States (Article 216(2) TFEU). According to settled case law of the CJEU, international agreements to which the EU is a party form an "integral part" of the EU legal system.[41] Of all the provisions of the "mixed agreements", only those that are in the exclusive or shared competence of the EU fall into the EU legal order.[42]

In the hierarchy of EU law, international trade law is situated between EU primary law, such as the Charter and the founding Treaties, and EU secondary law, including EU regulations, directives and decisions. If a trade agreement contradicts EU secondary law, preference will be given to the meaning of the secondary law that is more consistent with the provisions of the agreement.[43] This is the doctrine of parallel interpretation, which ensures deference to the international obligations of the EU.

i. Principle of autonomy of the EU legal order

The case law of the CJEU, especially its 2008 landmark decision in the *Kadi I* case,[44] underscores the principle of autonomy of the EU legal order vis-à-vis international law, which should respect the constitutional values and internal division of competences in the EU.[45] The advisory opinion procedure provided for in Article 218(11) of the TFEU underscores that in case of incompatibility with EU primary law, an international agreement cannot take effect.

Safeguard 5
Principle of autonomy of EU legal order *(strong)*
Protects the constitutional values and internal division of competences in the EU from external legal orders.

39 See request for an opinion submitted by the European Parliament on 10 April 2015 to the CJEU on an envisaged agreement between Canada and the EU on the transfer and processing of Passenger Name Record (PNR) data, CJEU, opinion 1/15 (pending).

40 See annulment of Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the US on the processing and transfer of Passenger Name Record (PNR) data by Air Carriers to the US Department of Homeland Security, CJEU, joined cases C-317/04 and C-318/04 (*European Parliament v. Council and Commission*), judgement of 30 May 2006, ECLI:EU:C:2006:346.

41 CJEU, case 181/73 (*Haegemann*), judgement of 30 April 1974, [1974] ECR 449, para. 5; opinion 1/91 (*EEA Agreement 1*), 14 December 1991, [1991] ECR 6079, para. 37.

42 Szilard Gaspar-Szilagyi, "The "Primacy" and "Direct Effect" of EU International Agreements", [2015], *European Public Law* 21(2), pp. 343-370, p. 350.

43 CJEU, case C-61/94 (*Commission v Germany*), judgement of 10 September 1996, [1996], ECR I-3989, para. 52.

44 CJEU, joint cases C-402/05 P and C-415/05 P (*Kadi I*), judgement of 3 September 2008, ECLI:EU:C:2008:461, paras. 282, 307, 308, 316.

45 Grainne de Burca, "The European Court of Justice and the International Legal Order After Kadi", [2010], *Harv. Int'l L.J.* 51(1), pp. 1-49, p. 5.

Moreover, the CJEU protects the exclusivity of its powers to interpret, enforce and invalidate EU law (Articles 263-267 TFEU).[46] The CJEU has repeatedly clarified that the exclusivity of its powers does not in principle eliminate the possibility of submitting the EU institutions to the interpretation of an international agreement by a court established or designated by that agreement.[47] However, such an international agreement cannot affect the essential character of the court's powers, and consequently adversely affect the autonomy of the EU legal order, which is safeguarded by the Court.[48]

The autonomy of the EU legal order requires an interpretation of fundamental rights within the framework of the structure and objectives of the EU.[49] Under this paradigm, it should not be possible for a court outside the institutional structure and judicial framework of the EU to bind the EU to particular interpretations of EU law.[50]

The principle of autonomy of the EU legal order, moreover, resolves that international agreements concluded by the EU fully supersede the national law of the Member States, including the principles and provisions of their constitutions.[51] In a similar vein, international agreements concluded by the EU would also supersede international obligations undertaken by Member States (Art 351 TFEU).

ii. Lack of direct effect

In EU law, the CJEU leverages the concept of "direct effect" as an argument for the preservation of the autonomy of the EU legal order vis-à-vis international law. Direct effect means that individuals and legal entities can directly invoke rights from an international agreement, or apply in national courts to invalidate EU secondary law based on its inconsistency with the international provisions. Conversely, without direct effect, judicial redress cannot be founded on provisions in international law.

To determine whether an international agreement has direct effect, the CJEU first inquires whether the parties to the international agreement at hand have agreed on the effect of the agreement in their internal legal orders.[52] Second, if the parties did not make such a determination in the agreement, the CJEU considers whether the nature and broad logic of the agreement does not preclude its direct application, and whether the content of the relevant provisions is "unconditional and sufficiently precise so as to confer on persons subject to European Union law the right to rely thereon in legal proceedings".[53] In the case law of the CJEU, the doctrine has been used to argue both in favour and against the direct effect of international law.

Safeguard 6
Absence of direct effect *(strong)*
In EU law, free trade agreements are not self-executing and do not directly confer rights on individuals and legal entities.

International trade agreements tend not to have direct effect on the grounds that they are not self-executing and do not directly confer rights on individuals and legal entities. This increasingly already follows from Council decisions to conclude international trade agreements. A study of post-2008 free trade agreements concluded by the EU shows that it has become a remarkable feature to include a so-called "no direct effect" clause in the agreement.[54] No direct effect clauses can appear in four different modalities:

46 CJEU, Opinion 2/13, (*Accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms*), 18 December 2014, ECLI:EU:C:2014:2454, paras. 170, 174.
47 Ibid., para. 182.
48 Ibid., paras. 183, 201.
49 Ibid., para. 170.
50 Ibid., paras 183-4; See also CJEU, opinion 1/09, (*Creation of a unified patent litigation system*), 8 March 2011, 2011 ERC I-01137, para. 76.
51 CJEU, case 11/70 (*Internationale Handelsgesellschaft*), judgement of 17 December 1970, [1970] ECR 1125, para. 3; C-399/11, (*Stefano Melloni v Ministerio Fiscal*), judgement of 26 February 2013, ECLI:EU:C:2013:107, para. 59.
52 CJEU, case C-366/10 (*Air Transport Association of America*), judgement of 21 December 2011, ERC I-13755, para. 49.
53 Ibid., para. 74.
54 See Aliki Semertzi, "The Preclusion of Direct Effect in the Recently Concluded EU Free Trade Agreements", (2014) *Common Market Law Review* 51(4), pp. 1125– 1158, p. 1127.

1. As a general clause in the agreement, precluding direct effect of the agreements;
2. As a clause that the ruling under the dispute settlement system does not create rights and obligations for natural or legal persons;
3. As a clause in the schedules of commitments; and
4. As a provision in the approving council decision.[55]

For example, the Council decision approving the WTO Agreement and its Annexes, including the GATS, reserves that "by its nature, the Agreement … is not susceptible to being directly invoked in [EU] or Member State courts".[56] CETA also includes such a provision in Article 30.6(1), according to which the agreement does not confer rights or impose obligations on persons other than the parties to the agreement under public international law. The provision also excludes the possibility of directly invoking the agreement in the domestic legal systems of the parties. Article 30.6(2) obliges each party not to provide a right of action under its domestic law against the other party to the agreement on the ground that a measure of the other party is inconsistent with the agreement.

Attention should be paid that international trade law still under negotiation, such as the TiSA and TTIP, contain similar "no direct effect" clauses, preferably in the agreement itself (first modality) and in the approving Council decision (fourth modality).

In any case, the CJEU is likely to conclude on the absence of direct effect of international trade agreements, analogue to its rulings on the General Agreement on Tariffs and Trade (GATT 1994), as well as its predecessor (GATT 1947). In the case of the GATT (1947), the CJEU rejected direct effect, arguing that the agreement is characterised by the "great flexibility of its provisions, in particular those conferring the possibility of derogation, the measures to be taken when confronted with exceptional difficulties and the settlement of conflicts between contracting parties".[57] The CJEU also concluded that the GATT rules are not unconditional, as it gives a contracting party power to unilaterally suspend the obligation and to withdraw or modify the concession.[58]

The only exceptions in which the CJEU agreed to review the conformity of EU secondary law in the light of an international agreement (GATT) have been cases where: 1) the EU intended to implement a particular obligation entered into within the framework of the GATT, or 2) if the Community act expressly refers to specific provisions of GATT (the so-called *Nakajima* and *Fediol* exceptions).[59] In subsequent cases, the CJEU interpreted these exceptions narrowly as applicable only to specific measures of the WTO (anti-dumping, anti-subsidies and trade barriers), and not applicable when reviewing secondary EU law for its conformity with the international agreement.[60]

The absence of direct effect in the international trade agreements cannot be overcome by the direct invocation of the decisions of dispute settlement bodies if these are established under the trade agreements. In the *FIAMM* case, the CJEU held that the decision of the WTO Dispute Settlement Body does not have direct effect essentially because the WTO agreements do not have direct effect. Granting direct effect to the decisions of the adjudicative bodies applying the WTO agreements would mean granting direct effect to the agreements themselves, which would contradict settled case law of the CJEU.[61]

55 Ibid., p. 1129.
56 Council Decision 94/800/EC of 22 December 1994 concerning the conclusion on behalf of the European Community, as regards matters within its competence, of the agreements reached in the Uruguay Round multilateral negotiations (1986-1994).
57 CJEU, case C-122/95 (*Germany v Council*), judgement of 10 March 1998, ECR I-00973, para. 106.
58 Ibid., paras 108, 110.
59 Ibid., para. 111 referring to CJEU, case 70/87 (*Fediol v Commission*), judgement of 22 June 1989, ECR 1781 and Case C-69/89 *(Nakajima v Council*), judgement of 7 May 1991, ECR I-2069.
60 Gaspar-Szilagyi (fn. 42), p. 361.
61 CJEU, case C-120/06 P (*FIAMM v. Council*), judgement of 9 September 2008, ECR I-06513, paras 125-128.

iii. Legal consequences

International trade law is not self-executing in the EU legal order, but requires the EU to adopt legislative measures for compliance.[62] The legal consequences safeguard EU law from becoming automatically invalidated by international trade law. Even though both international trade agreements and decisions of the dispute settlement bodies are legally binding under public international law, this binding effect is substantially mitigated by the principle of the autonomy of the EU legal order.

Without direct effect, the EU enforcement mechanism for international trade agreements and decisions of the dispute settlement bodies established under such agreements is sufficiently weakened. Private parties cannot directly invoke provisions from international trade law to override EU secondary law in EU or Member State courts. Furthermore, private parties cannot sue EU institutions for non-contractual damages caused to them by the EU's non-compliance with international trade law under Articles 268 and 340 of the TFEU.

62 E.g. EU Regulation No. 912/2014 of the European Parliament and of the Council of 23 July 2014 establishing a framework for managing financial responsibility linked to Investor-to-State Dispute Settlement tribunals established by international agreements to which the European Union is party, [2014] Official Journal L 257/121.

III. International trade law with EU participation

This chapter covers the international trade and investment law to which the EU is a party, or on which the EU is in the process of negotiating an agreement. It covers the GATS and its potential successor TiSA, as well as CETA and TTIP. These instruments are briefly introduced in order to set the scene for the legal assessment in Chapter IV and the comparative analysis in Chapter V.

International trade in services and investment treaties can broadly be distinguished according to whether they are multilateral or bilateral agreements. The GATS and its potential successor TiSA, on the one hand, fall into the category of multilateral agreements. CETA and TTIP, on the other hand, are bilateral agreements to which the EU would become a party.[63]

Another distinction is based on the scope of the agreement: whether it only covers trade in services, or also includes investment protection. In this regard, the GATS is a stand-alone instrument that aims to liberalise trade in services, whereas CETA, TTIP and TiSA will additionally comprise investment protection.

In the next section, the GATS and CETA are introduced first as the texts of the agreements are fully documented. Free trade agreements still under negotiation follow, i.e. TTIP and TiSA. It is important to bear in mind that negotiations have not been concluded in these cases, and thus the final texts of the relevant provisions are not available. The assessment and the comparative analysis in Chapter V is based on a combination of the official documentation and position papers of the Commission but also – in the absence of full transparency – on unofficial releases of so-called bracketed drafts.[64]

1. General Agreement on Trade in Services (GATS)

The GATS is the first multilateral treaty on the liberalisation of international trade in services. It forms part of the 1994 Marrakesh Agreement on Establishing the World Trade Organisation (WTO Agreement) as Annex 1B.[65] Annex 1 in this document reproduces the relevant provisions of the GATS.

The primary aim of the GATS is the expansion of international trade in services through the elimination of trade barriers. The preamble to the GATS also acknowledges the right of WTO Member States to regulate in order to pursue their national policy objectives.[66] Nevertheless, national regulation affecting trade in services must be consistent with the GATS and applied non-discriminatorily (GATS Articles VI(1) and XIV(c)).

The GATS applies to "any service in any sector" (GATS Article I(3)(b)) with the exception of services supplied in the exercise of governmental authority.[67] The GATS covers "trade in services" in four modes of supply: cross-border supply (mode 1), consumption abroad (mode 2), commercial presence (mode 3), and presence of natural persons (mode 4).[68]

The GATS provides for general obligations and specific commitments. The core general obligation is Most-Favoured-Nation (MFN) treatment (GATS Article II), which is automatically and unconditionally binding unless a WTO member has chosen unbound or

63 The EU and its Member States could also conclude them as so-called "mixed agreements".
64 Bracketed drafts contain negotiation positions of the countries and signify where there are different textual proposals. Hence, bracketed drafts should not be read as if they are already agreed upon, and EU proposals are labelled as such.
65 WTO, General Agreement on Trade in Services (GATS), available at <https://www.wto.org/english/docs_e/legal_e/26-gats.pdf> (accessed 10 May 2016).
66 Recital 3 of the Preamble to the GATS.
67 Article I:3 of the GATS.
68 Article I:2 of the GATS.

has listed reservations in its schedule of commitments (GATS Article II). GATS Article VI on domestic regulation is the other obligation.

The most important specific commitments are market access and national treatment (GATS Articles XVI and XVII). Specific commitments become binding only if and to the extent that the member country has indicated this in its schedule of specific commitments. These schedules constitute an integral part of the GATS (GATS Article XX:3) and of the member's WTO accession package.

The GATS also set the schedule for negotiations on the progressive liberalisation of services in the aftermath of the Uruguay Round. The Understanding on Commitments in Financial Services laid the basis for further liberalisation in this sector.[69] Negotiations resulted in two new annexes covering basic telecommunications and financial services.[70]

The general exceptions under GATS Article XIV hold an affirmative defence by acknowledging the right of WTO members to pursue public interest objectives by adopting and enforcing measures inconsistent with any obligation under the GATS.

The GATS is enforced exclusively through the WTO government-to-government enforcement mechanism: the Dispute Settlement System (DSS).[71] The WTO panels and Appellate Body (the WTO adjudicating bodies) treat WTO jurisdiction as autonomous.[72]

Both the EU and its Member States are original parties to the GATS and the WTO alike. The EU is bound by all general obligations under the GATS. In its services schedules, the EU specifies in which sectors, in relation to which modes of supply, and to what extent it shall be bound by market access and national treatment obligations.[73]

2. Comprehensive Economic and Trade Agreement (CETA)

The Comprehensive Economic and Trade Agreement (CETA) is a bilateral free trade agreement between the EU and Canada. Negotiations of the treaty finished in August 2014 with the approval of the final text of the agreement. The text of the agreement was published after legal review by the Canadian Government and the Commission.[74] The relevant provisions of CETA are reproduced in Annex 1.

The EU legislator has not yet formally adopted CETA. In June 2016, the Commission will submit a proposal to the Council for the signature and provisional application of CETA. The plan is to sign CETA at an EU-Canada Summit in October 2016.[75] For the time being, the agreement is not binding under international law.

---

69 The understanding is not a part of the GATS, but is an appendix to the Final Act of the Uruguay Round, available at <www.wto.org/english/tratop_e/serv_e/finance_e/finance_e.htm> (accessed 8 April 2016).

70 Annex on Telecommunications and Annex on Financial Services.

71 Peter van den Bossche and Werner Zdouc, *The Law and Policy of the World Trade Organization: Text, Cases and Materials* (Cambridge: CUP, 2013, third ed.), p. 161.

72 Mitsuo Matsushita, Thomas J. Schoenbaum and Petros C. Mavroidis, *The World Trade Organization: Law, Practice, and Policy* (Oxford: OUP, 2006), pp. 79-80.

73 Consolidated GATS Schedule (EU-25), 9 October 2006, available at <http://trade.ec.europa.eu/doclib/docs/2008/september/tradoc_140355.pdf>; the convolute of EU schedules of specific commitments, including supplements and revisions, is available via the WTO document centre at <https://docs.wto.org/>.

74 Comprehensive Economic and Trade Agreement (CETA) between Canada, of the one part, and the European Union [and its Member States], available at <http://trade.ec.europa.eu/doclib/docs/2016/february/tradoc_154329.pdf> (accessed 20 April 2016).

75 Council of the European Union, "Foreign Affairs Council – Trade Issues, Friday 13 May in Brussels", press release of 11 May 2016, available at <http://www.consilium.europa.eu/en/meetings/fac/2016/05/Background-Trade-160513_pdf/> (accessed 14 May 2016).

The Council's negotiation mandate holds no mention of privacy or data protection.[76] It should be recalled that Commission Decision 2002/2/EC found that Canada has an adequate level of protection pursuant to the DPD.[77] This permits personal data from the EU to be transferred to Canada without any additional safeguards.

CETA is a comprehensive agreement in the sense that it covers most sectors and aspects of Canada-EU trade. In relation to trade in services, the scope of the agreement has been broadened by new and enhanced disciplines. CETA contains separate chapters on cross-border trade in services, investment (including investor protection), financial services, telecommunications and e-commerce. The chapters on financial services, telecommunications, electronic commerce and regulatory co-operation contain special provisions on privacy and data protection.

Chapter 28 Article 3 on "Exceptions" provides for general exceptions that would apply to the relevant chapters on cross-border trade in services, domestic regulations, financial services, telecommunications, electronic commerce and investment. The wording of this exception is almost identical to that of GATS Article XIV.

CETA includes a general inter-state dispute settlement mechanism that will be used for the resolution of disputes between parties concerning the interpretation and application of CETA (Chapter 8). Moreover, CETA establishes an Investor-to-State Dispute Settlement (ISDS) mechanism in order to enforce obligations of the parties on non-discriminatory treatment and investor protection (Chapter 8, Section F, Article 18).[78] The agreement introduces institutions and procedures for regulatory co-operation.

Article 30.6 of CETA holds a "no direct effect" clause, which would be effective in EU law in preventing private legal actions directly invoking the agreement.

3. Transatlantic Trade and Investment Partnership (TTIP)

The Transatlantic Trade and Investment Partnership (TTIP) is a so-called "mega-regional" free trade agreement negotiated between the EU and the US. TTIP is intended as a companion agreement of the Trans-Pacific Partnership (TPP) concluded between the US and Asia-Pacific countries. Negotiations on TTIP started in July 2013.

a. Negotiation mandate

TTIP is negotiated by the Commission on behalf of the EU, on the basis of negotiation directives from the Council.[79] The negotiation mandate does not mention privacy or data protection. It does request that the Agreement not preclude the enforcement of exceptions on the supply of services justifiable under the relevant WTO rules (GATS Articles XIV and XIV *bis*). However, the negotiation mandate covers information and communication technologies and financial services, and aims to remove existing non-tariff barriers, prevent the introduction of new non-tariff barriers, and allow market access at a level greater than that delivered through horizontal rules.[80]

---

76 Council of the European Union, document 9036/09 (partially declassified), available at <http://data.consilium.europa.eu/doc/document/ST-9036-2009-EXT-2/en/pdf> (accessed 20 April 2016).

77 Commission, Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act [2001], Official Journal L 2/13.

78 Recently, the Commission is looking into the possibility to replace ISDS with a dedicated Investment Court System, see Commission, "CETA: EU and Canada agree on new approach on investment in trade agreement", press release of 29 February 2016, available at <http://europa.eu/rapid/press-release_IP-16-399_en.htm> (accessed 10 May 2016).

79 The Council of the European Union, Directives for the negotiation on the Transatlantic Trade and Investment Partnership between the European Union and the United States of America 11103/13 of 17 June 2013, available at <http://data.consilium.europa.eu/doc/document/ST-11103-2013-DCL-1/en/pdf> (accessed 20 April 2016).

80 Ibid., Article 25.

In its 2015 resolution on TTIP, the European Parliament called on the Commission to ensure that the EU's acquis on data privacy is not compromised through the liberalisation of data flows, in particular in the areas of e-commerce and financial services. [81] A key point of the Parliament resolution is the call for a comprehensive and unambiguous horizontal self-standing provision, based on GATS Article XIV, that fully exempts the existing and future EU legal framework for the protection of personal data from the agreement, without any condition that it must be consistent with other parts of TTIP.[82]

b. Documentation

Following criticism about the secrecy surrounding the TTIP negotiations, the Commission changed its practice and now publishes its textual proposals to the US. This included the proposal for a Title on trade in services, investment and e-commerce in July 2015, as well as accompanying documents such as summaries of the negotiation rounds and other explanatory documents. The bracketed drafts of the agreement, which would reveal the negotiating positions of the US, are not part of the Commission's transparency initiative.

In May 2016, an entire TTIP draft dated 30 November 2015 was unofficially released.[83] The document contains, among other items, the bracketed drafts of the chapters on cross-border trade in services, electronic communications/telecommunications, regulatory co-operation, and a document entitled Tactical State of Play. There is consistency between the textual proposals of the Commission and the EU proposals in the bracketed draft TTIP text.

Some newer EU positions were not yet reflected in the unofficially released TTIP draft, and have therefore been added to the documentation upon which this study is based. For example, the Commission proposes a new approach to investment protection championing a permanent investment court system instead of the Investor-to-State Dispute Settlement system.[84] Additionally, the Commission's new position aims to enshrine governments' right to regulate.

The comparative overview in Annex 1 reproduces the publicly accessible relevant provisions of the TTIP negotiations that were available when this study was published.

c. Substance

The ambition of the parties is to establish deeper trade integration in comparison to the GATS system, while remaining consistent with WTO rules and obligations.[85] TTIP is based on three pillars: market access for goods and services, regulatory co-operation (including regulatory coherence and technical standards) and rules (including investment, competition, intellectual property and government-to-government dispute settlement).

---

81 European Parliament, Resolution of 8 July 2015 containing the European Parliament's recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP), adopted 8 July 2015, para. (xii), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0252+0+DOC+XML+V0//EN> (accessed 10 May 2016).

82 Ibid.

83 Greenpeace Netherlands, TTIP Leaks, May 2016, available at <https://www.ttip-leaks.org/> accessed 10 May 2016; see Commission, "Negotiating TTIP: Comment by Commissioner Malmström", Brussels, 2 May 2016, available at <http://trade.ec.europa.eu/doclib/press/index.cfm?id=1492> accessed 10 May 2016.

84 Commission, "Commission proposes new Investment Court System for TTIP and other EU trade and investment negotiations", Brussels, 16 September 2015 <http://europa.eu/rapid/press-release_IP-15-5651_en.htm> (accessed 10 May 2016); Commission, Proposal TTIP Trade in services, investment and e-commerce, Chapter II Investment, 16 September 2015, available at <http://trade.ec.europa.eu/doclib/docs/2015/september/tradoc_153807.pdf> (accessed 10 May 2016).

85 Ibid.

The draft chapter on cross-border trade in services covers the four core disciplines of free trade: MFN treatment, domestic regulation, market access and national treatment. TTIP envisages a range of new and enhanced disciplines, notably service chapters on financial services, electronic communications/telecommunications, and electronic commerce including computer services. Presently, only the chapters on financial services and electronic communications/telecommunications are maturing.

The Commission and the leaked TTIP Tactical State of Play document unanimously report that the issue of privacy and data flows is unresolved. The Commission states that "once the privacy issues on transatlantic data flows are resolved we will also be in a position to advance on digital services...".[86] The Tactical State of Play document reveals that "[d]iscussions on e-commerce covered all proposals except for the provisions on data flows and computing facilities."[87]

EU proposals aim for horizontal provisions in TTIP holding the right to regulate and a general exception for measures of public interest.[88]

The EU's negotiation position on cross-border trade in services contains a right to regulate, pursuant to which each party retains the right to adopt, maintain, and enforce the measures necessary to pursue legitimate policy objectives, consistent however with the core disciplines. The EU proposal also surfaces in the leaked TTIP drafts.

The EU proposes a general exception from the application of the specified provisions of the Title on trade in services, investment and e-commerce, which is almost identical to Article XIV of the GATS. Most importantly, this TTIP Article sets forth the same test for applicability of the exception to particular rules and regulations.

The EU proposals on TTIP include a chapter on a government-to-government dispute settlement mechanism in connection with the application and interpretation of the agreement.[89] The latest proposal on an investment court system supersedes an older EU proposal on investment protection.[90]

At the moment, there is no sign of a "no direct effect" clause. This may however just be a reflection of the state of negotiations and the publicly available documents.

4. Trade in Services Agreement (TiSA)

The Trade in Services Agreement (TiSA) is being negotiated by the EU, the US and 21 other members of the WTO, which collectively account for about 70 percent of world

86 Commission, The Transatlantic Trade and Investment Partnership (TTIP) – State of Play, 27 April 2016, p. 4, available at <http://trade.ec.europa.eu/doclib/docs/2016/april/tradoc_154477.pdf> (accessed 10 May 2016).

87 Anon., "Note-Tactical State of Play of the TTIP Negotiations", March 2016, p. 7, available at <https://www.ttip-leaks.org> (accessed 10 May 2016).

88 Commission, EU proposal for services, investment and e-commerce text, 31 July 2015, fn. 21, available at <http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153669.pdf> (accessed 10 May 2016). This proposal was tabled for discussion with the US in the negotiating round of 12 -17 July 2015. The actual text in the final agreement will be a result of negotiations between the EU and the US.

89 Commission, EU initial proposal for legal text on "Dispute Settlement (Government to Government)" in TTIP. It was tabled for discussion with the US in the negotiating round of 10-14 March 2014 and made public on 7 January 2015, available at <http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_153032.pdf> (accessed 20 April 2016). The actual text in the final agreement will be a result of negotiations between the EU and the US.

90 Commission, EU proposal for Investment Protection and Resolution of Investment Disputes. It was tabled for discussion with the US and made public on 12 November 2015, available at <http://trade.ec.europa.eu/doclib/docs/2015/november/tradoc_153955.pdf> (accessed 20 April 2016). The actual text in the final agreement will be a result of negotiations between the EU and the US.

trade in services.[91] The negotiation parties view TiSA as an instrument to move forward the multilateral trade negotiations that have been stalled in the WTO system, largely due to the required unanimity in decision making on trade rules.

a. Negotiation mandate

TiSA negotiations started in September 2013. The negotiating directives for a plurilateral Trade in Services Agreement were published in June 2015.[92] While guidelines on privacy and data protection are not included, the Council's mandate holds that negotiations should aim at including telecommunication services, computer-related services, e-commerce, cross-border data transfers, financial services, and postal and courier services.[93]

In its 2016 resolution, the European Parliament calls on the Commission to negotiate TiSA rules on the digital economy prudently, especially where they touch upon privacy and data protection rights as guaranteed in EU law.[94] In particular, the European Parliament stresses that EU negotiators should reject "any "catch-all" provisions on data flows which are disconnected from any reference to the necessary compliance with data protection standards."[95] The resolution continues by stating that data protection and the right to privacy are not trade barriers, but fundamental rights. The European Parliament call is similar to its TTIP resolution:

> [A] comprehensive, unambiguous, horizontal, self-standing and legally binding provision based on GATS Article XIV which fully exempts the existing and future EU legal framework for the protection of personal data from the scope of this agreement, without any conditions that it must be consistent with other parts of the TiSA; to apply such provisions to all other TiSA annexes; ...[96]

b. Documentation

In 2013, the Commission distributed its proposal for the core TiSA text provisions[97] and for an Annex on Financial Services.[98] The overall negotiating process is not fully transparent. In 2015, a newer version of the core text provisions and annexes on electronic commerce and telecommunications appeared on Wikileaks. This study refers to these leaked documents and to the official EU proposal for an Annex on Financial Services.

According to the Commission, the objective of the 16th TiSA negotiation round that took place in early 2016 was to get closer to agreeing on text in all annexes on digital issues (telecoms, e-commerce and localisation).[99] TiSA participants committed on a revised

---

91 Australia, Canada, Chile, Chinese Taipei, Colombia, Costa Rica, the EU, Hong Kong China, Iceland, Israel, Japan, Korea, Liechtenstein, Mauritius, Mexico, New Zealand, Norway, Pakistan, Panama, Peru, Switzerland, Turkey and the US; see Commission's website at <http://ec.europa.eu/trade/policy/in-focus/tisa/> (accessed 10 May 2016).

92 Council of the European Union, Draft Directives for the negotiation of a plurilateral agreement on trade in Services, 10 March 2015, para. 7, available at <http://data.consilium.europa.eu/doc/document/ST-6891-2013-ADD-1-DCL-1/en/pdf> (accessed 20 April 2016).

93 Ibid.

94 European Parliament (fn. 1).

95 Ibid., para. (c).iv.

96 Ibid., para. (c).iii.

97 Commission, Plurilateral Service Agreement ‚Draft Text Provisions, March 2013, available at <http://trade.ec.europa.eu/doclib/docs/2014/july/tradoc_152687.pdf> (accessed 20 April 2016). The actual text in the final agreement will be a result of negotiations between the EU and other parties to the negotiations.

98 Commission, TiSA Financial Services, March 2013, available at <http://trade.ec.europa.eu/doclib/docs/2014/july/tradoc_152688.pdf> (accessed 20 April 2016). The actual text in the final agreement will be a result of negotiations between the EU and other parties to the negotiations.

99 Commission, Report of the 16th TiSA negotiation round, 19 February 2016, p. 2, available at <http://trade.ec.europa.eu/doclib/docs/2016/february/tradoc_154306.doc.pdf> (accessed 10 May 2016).

work plan that aims to have the content of the key annexes agreed by July 2016 and the remaining texts by September 2016.

It can therefore be assumed that drafts have matured from the documentation this study is based on. Annex 1 reproduces the provisions of the TiSA negotiations that were publicly accessible when this study was published.

c. Substance

TiSA is largely based on the GATS, and incorporates its key provisions on scope, definitions, market access, national treatment and exemptions. In comparison with the GATS, TiSA will likely contain provisions on deeper trade integration between the parties, including regulatory disciplines on transparency, telecommunication services and e-commerce. TiSA is open to all WTO Member States. It is anticipated that TiSA will eventually be integrated with or supersede the GATS.[100]

The intertwined issues of data flows, privacy and data protection are very salient topics in TiSA negotiations. On the one hand, parties to TiSA negotiations (although not the EU) attempt to inject positive obligations for the adoption or maintenance of a personal information protection framework. The annexes on telecommunications, electronic commerce (which at the moment consists of a set of proposals by negotiating parties), and financial services contain specific provisions aimed at safeguarding privacy and data protection.

On the other hand, proposals in the annexes on financial services and electronic commerce aim for commitments on cross-border information flows. The Commission reports that discussions on data flows and the location of computing facilities (issues on which the EU has not yet actively engaged) have thus far not yielded much progress.[101] However, several participants pointed to the need for strong exceptions for public policy objectives if these provisions are included in the final TiSA text. Article I-9 of the TiSA core text provisions literally reproduces the GATS Article XIV general exceptions, which appear to be less controversial.

TiSA will certainly come with a government-to-government dispute settlement system, which will be defined at a later stage.[102] Whether the agreement will also contain an investor-to-state dispute settlement mechanism is unclear from the documents. EU officials declared publicly that this is not the intention of the EU nor of the other TiSA partners. There is also no clarity on whether the EU will inject a "no direct effect" clause into TiSA.

A few initial observations can be drawn following the introduction of the four international trade agreements covered by this study (the GATS, CETA, TTIP and TiSA). At first glance, in comparison with the GATS, newer free trade and investment treaties are characterised by one or more of the following elements: new and enhanced disciplines, especially e-commerce; GATS-plus liberalisation ambitions in the schedules of commitments, and investment protection as well as regulatory co-operation.

100 Council of the European Union, Draft Directives for the negotiation of a plurilateral agreement on trade in services, 10 March 2015, para. 7, available at <http://data.consilium.europa.eu/doc/document/ST-6891-2013-ADD-1-DCL-1/en/pdf> (accessed 20 April 2016).

101 Commission, Report of the 16th TiSA negotiation round (fn. 99), p. 2.

102 Ex-TiSA chief negotiator Ignacio Iruarrizaga during a civil society dialogue meeting in December 2015 in Brussels.

IV. Assessment of EU data protection law under the GATS

In this section, the GATS is applied to EU data protection law and implementation measures. This exercise is an important interim step before embarking on the comparative analysis of newer international trade agreements that incorporate similar commitments, namely the CETA, TTIP and TiSA, and before determining the extent and effect of new and enhanced disciplines in the services schedules on financial services, telecommunications/electronic communications and e-commerce.

Through this application, it is possible to lay an understanding for the core disciplines and to clarify whether an EU measure in the field of data protection might be in conflict with existing GATS obligations and commitments. The analysis then turns to possible justifications under the GATS, namely in its Articles V and XIV. This approach reproduces the internal logic of the GATS, in which the reliance on justifications and exceptions is necessary only when there has first been a violation of the GATS.

In approaching the hypothetical analysis under the GATS, it is imperative to ascertain whether the measure to which the GATS is applied concerns EU legislation, i.e. the DPD today and the GDPR in the near future, or a decision by a competent authority based on EU data protection law. The latter is best illustrated by the decisions of the Commission attesting to the adequate level of protection in a third country based on the rules on transfer of personal data to third countries (Article 25(6) DPD). As implementation measures, the Commission's adequacy decision – to stay with this example – could be the subject of a complaint under the WTO DSS without challenging the underlying EU legislation.

1. Caveats

This hypothetical analysis is informed by WTO law, the jurisprudence of WTO adjudicating bodies, and literature.[103] To date, there has never been a WTO procedure challenging a member's measure that puts privacy and data protection legislation to the test. Hence, this study offers a legal assessment without relying on any concrete precedent, and further legal insecurity persists owing to the fact that WTO adjudicating bodies have a certain margin of interpretation that cannot be fully anticipated.

This analysis is informed by four reports of the WTO Appellate Body, including the most recent report in the *Argentina – Measures relating to trade in goods and services* case, which illustrate how the GATS is interpreted and applied.[104] It is noteworthy that two of the GATS cases already interrogate cross-border data flows, in particular the supply of online gambling to the US and the electronic wholesale distribution of content to the

103 Van der Bossche and Zdouc (fn. 71); William J. Drake and Nicolaïdis Kalypso, "Global Electronic Commerce and GATS: The "Millennium Round" and Beyond," in: GATS 2000: New Directions in Services Trade Liberalization, (P. Sauve and R. M. Stern, eds., Washington DC: The Brookings Institution Press, 2000), pp. 399-437; Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford: OUP, 2013); Carla L. Reyes, "WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive", [2011], *Melbourne Journal of International Law* 12, pp. 2-36; Gregory Shaffer, "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of US Data Privacy Standards", [2000], *Yale Journal of International Law* 25, pp. 1-88; Eric Shapiro, "All Is Not Fair in the Privacy Trade: The Safe Harbor Agreement and the World Trade Organization", [2003], *Fordham Law Review* 71(6), pp. 2781-2821; Rolf H. Weber, "Regulatory Autonomy and Privacy Standards under the GATS", [2012], *7 Asian Journal of WTO & International Health Law & Policy*, pp. 25-48.

104 WTO Appellate Body Reports, *European Communities – Regime for the Importation, Sale and Distribution of Bananas (Bananas III),* (WT/DS27/AB/R 9 September 1997); *US – Measures affecting the cross-border supply of gambling and betting services,* (WT/DS285/AB/R, 7 April 2005); *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products,* (WT/DS363/AB/R 21 December 2009); *Argentina – Measures relating to trade in goods and services,* (WT/DS453/AB/R 14 April 2016).

Chinese market.[105] This would support the relevance of WTO jurisprudence in trade conflicts in relation to electronic commerce, and inter alia measures regulating the processing of personal data.[106]

2. Jurisdiction

The GATS is enforced exclusively through the WTO Government-to-Government Dispute Settlement System (DSS). In the system of public international law, WTO law is *lex specialis* owing to its own enforcement mechanism and remedies for breach. The WTO panels and Appellate Body (WTO adjudicating bodies) are generally reluctant to apply non-WTO law in dispute settlement proceedings. This is important, as WTO adjudicating bodies are in their interpretation not bound by the interpretations of measures in the context of a legal system or court rulings, such as the CJEU.

3. Scope and definitions

The scope of the GATS is defined in its Article I. The GATS applies to "measures affecting trade in services" in one or several modes of supply. Measures broadly covers legislation and executive acts in the exercise of public authority by government at any level and by non-governmental bodies exercising delegated authority (GATS Article I:3(a)).[107]

The digital economy and online trade in services postdate the GATS, and a substantial lack of clarity persists as to how the sectors governed by the WTO and provisions of the GATS will be interpreted and applied.[108] Without hesitation, however, the WTO Appellate Body report in *US - Gambling* in principle resolved that the GATS applies to services delivered electronically.[109] This means that WTO jurisdiction extends to electronic services, where personal data processing is oftentimes inextricably intertwined with the ordinary conduct of business.

Beyond doubt, EU data protection law has an effect on international trade, not least because it regulates certain instances of the cross-border processing of personal data and contains provisions on the transfer of personal data to third countries (see Section II.2).[110] The provisions of the DPD itself, and all implementing acts of the Commission and Member States' national data protection authorities, are susceptible to appraisal under the GATS. Potentially, these measures can simultaneously affect cross-border supply (mode 1), consumption abroad (mode 2), and commercial presence (mode 3).

Risk IV
Personal data processing is inextricably intertwined with the ordinary conduct of business *(strong)*
Potentially, trade disputes can arise in any sector covered by a party's schedules of commitments.

4. Obligations and commitments

The GATS provides for two general obligations, namely Most-Favoured-Nation (MFN) treatment (GATS Article II) and domestic regulation (GATS Article VI), and specific commitments, the most important of which are market access (GATS Article XVI) and national treatment (GATS Article XVII).

105 Susan A. Aaronson, "The Digital Trade Imbalance and Its Implications for Internet Governance," 2016 Global Commission on Internet Governance Paper Series No. 25, p. 6, available at <https://www.cigionline.org/publications/digital-trade-imbalance-and-its-implications-internet-governance> (accessed 10 May 2016).

106 Mira Burri, "Should There Be New Multilateral Rules for Digital Trade?", Think piece for the E15 Expert Group on Trade and Innovation (Geneva: International Centre for Trade and Sustainable Development, 2013), p. 2, available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2344629> (accessed 10 May 2015); Sacha Wunsch-Vincent, "Trade Rules for the Digital Age", in: *GATS and the Regulation of International Trade in Services* (M. Panizzon, N. Pohl, and P. Sauvé, eds., Cambridge: CUB, 2008), pp. 497-529.

107 Except services supplied in the exercise of governmental authority (GATS Article I:3.(b) and (c)).

108 See Aaronson (fn. 105), p. 6; Burri (fn. 106), p. 2; Drake and Nikolaides (fn. 103), p. 431.

109 WTO Appellate Body Report, *US - Gambling* (fn. 104), paras 180f.

110 See Kuner (fn. 103), p. 52 and references in fn. 133.

a. Schedules of commitments

The GATS commitments must, as a rule, be read in conjunction with the EU's schedules of commitments. For example, the specific GATS commitments on market access and national treatment rest on positive lists, which means that a member does not undertake any commitment unless the sector is included in its schedules of specific commitments.[111] In the case of the MFN treatment obligation, GATS members had the chance to submit "exception lists" until the entry into force of the WTO agreement. GATS Article II exemptions take a negative list approach, but any changes would currently require a quorum of three-fourths of the members to be accepted.

The WTO Services Sector Classification List determines the structure of the schedules of commitments.[112] Neither processing of personal data nor privacy and data protection law are service sectors and, hence, the "positive list" approach cannot be used to avoid entering into commitments. Instead, personal data is processed in the course of supplying services in sectors, which are listed in the schedules of commitments. This, in turn, makes privacy and data protection standards susceptible to market liberalisation via free trade agreements.

The EU undertook specific commitments in modes of supply 1, 2 and 3 with respect to services that would involve the processing of personal data, such as for example data processing services, database services and other computer services (in the sector of computer and related business services),[113] telecommunications,[114] travel agencies and tour operators,[115] computer reservations systems,[116] and financial services (primarily insurance and banking).[117] For each of these services the EU entered a number of limitations, most of which however do not concern the processing of personal data.

In the past, the interpretation of the schedules of commitments has been contentious. The WTO adjudicating bodies can interpret the scope of the schedules autonomously. This can lead to an interpretation different than what the member country intended when entering into commitments to liberalise certain sectors.[118] Presumably, services that rely on the processing and transfer of personal data would automatically be subsumed under the service sector, even if it were defined offline or physically.

b. Most-favoured-nation treatment

Considered as the single most important rule in WTO law, MFN treatment provides:

> With respect to any measure covered by this Agreement, each Member shall accord immediately and unconditionally to services and service suppliers of

111 Commission, Services and investment in EU trade deals: Using "positive" and "negative" lists, April 2016, available at <http://trade.ec.europa.eu/doclib/docs/2016/april/tradoc_154427.pdf> (accessed 10 May 2016).

112 See WTO, Services Sector Classification List (MTN.GNS/W/120 10 July 1991); see for a critique of the service classification system in the digital economy Rolf H. Weber and Mira Burri, *Classification of Services in the Digital Economy*, Zurich: Schulthess, 2012, p. 38f.; Wunsch-Vincent (fn. 106), p. 502f.

113 EU Schedule of Specific Commitments (GATS/SC/31 15 April 1994), s. 1.II. B c), d) and e).

114 EU Schedule of Specific Commitments Supplement 3 (GATS/SC/31/Suppl. 3 11 April 1997), s. 2.C.

115 EU Schedule of Specific Commitments (fn 113), s. 9.B.

116 Ibid., s. 11.C.d.

117 EU Schedule of Specific Commitments Supplement 4 Revision (GATS/SC/31/Suppl.4/Rev.1 18 November 1999).

118 In *US – Gambling* (fn. 104), the WTO Appellate Body interpreted the entry in the schedules of commitments "Other recreational services (except sporting)" as covering gambling and betting services. Report of the Appellate Body (7 April 2005), WT/DS285/AB/R, paras 158f. In *China – Publications and audiovisual products* (fn. 104) the WTO panel concluded that the entry in the schedules of commitments on "sound recording distribution services" extends to the wholesale distribution of content via electronic means, paras. 36f.

> any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country. (GATS Article II.1)

The MFN obligation is automatically and unconditionally binding on each WTO member unless a WTO member has chosen unbound or listed reservations in its schedule of commitments (GATS Article II).

The principle goal of the MFN is equal opportunity to supply "like" services and, hence, the elimination of discrimination between the different trading partners of a WTO Member State.[119] Conversely, different treatment of services and service suppliers that are not "like" does also not constitute discrimination under MFN treatment obligation.

To ensure consistency of interpretation of the same terms in MFN and national treatment disciplines of the GATS, WTO adjudicating bodies apply the same tests for "likeness" and "no less favourable".

Hence, the key criteria for triggering the MFN treatment obligation are "like" services and service suppliers and "treatment no less favourable". Assessed on a case-by-case basis, services and service suppliers are "like" if they are "in a competitive relationship."[120] Services and service suppliers are presumed to be "like" if a measure differentiates by reason of origin ("presumption approach"),[121] unless it can be shown that such difference in treatment based on the regulatory framework is "inextricably linked to such origin".

The WTO Appellate Body's reading of "treatment no less favourable" is that "a measure accords less favourable treatment if it modifies the conditions of competition to the detriment of like services or service suppliers of any other Member."[122] Even if a measure does not distinguish, on its face, between domestic and foreign service suppliers, it may nevertheless amount to a treatment less favourable between foreign services and service suppliers. This is because contrary to the legal opinion of the (then) European Communities, the WTO Appellate Body held that MFN treatment covers formal and actual discrimination.[123]

Applied to EU data protection law, the DPD rules on transfer of personal data to third countries enshrine a differential treatment according to whether or not the country of destination of a personal data transfer ensures an adequate level of protection. While the third country of destination of personal data may coincide with the origin of the service and a service supplier, the difference in treatment is not "based exclusively on origin".[124]

Rather it is induced by other factors, i.e. the adequate level of protection afforded in a given third country that in turn is "inextricably linked to such origin".[125] In that case, in order to establish the "likeness", a more detailed analysis into the competitive relationship between the services and the service suppliers at issue would be required on a case-by-case basis.

When interrogating the "likeness" between comparable online services, the argument could be made that a high level of privacy and data protection is valued by the customers. For example, in business-to-business computer services, data localisation in Europe has

Risk V

EU rules on the transfer of personal data to third countries trigger non-discrimination commitments *(medium)*

Categorising third countries according to whether they afford an adequate level of protection or not would be found GATS inconsistent that needs to be justified.

119 The MFN treatment has been interpreted as banning both formal and informal discrimination, see WTO Appellate Body Report, *EC – Bananas III* (fn. 104), para. 234.

120 WTO Appellate Body Report, *Argentina – Measures relating to trade in Goods and Services* (fn. 104), para. 6.3.4.

121 Ibid., paras 6.29f.

122 Ibid., para. 6.129.

123 WTO, Appellate Body report, *EC – Bananas III* (fn. 104), para. 234.

124 Ibid., para. 6.60.

125 In relying on this "other factor", it must be demonstrated that it affects the competitive relationship between services and service suppliers, for example, by showing its effect on the characteristics of the service and on consumers' preferences. Ibid., para 6.6.

evolved into a recurrent requirement of enterprise customers.[126] Consumers, on the other hand, while clearly valuing privacy and data protection, often act irrationally (the so-called "privacy paradox") and online services can relatively easily influence consumer behaviour concerning their personal information.[127] Hence, for business-to-consumer markets, privacy and data protection can likely not yet be regarded a characteristic of a particular online service that would influence the outcome of "likeness".

The EU's rational for granting a more favourable regime to data transfers to third countries with an adequate level of protection is to prevent circumvention of its data protection framework by transferring personal data outside the EU. The DPD's rationale, however, would not in any way influence the appraisal of "treatment no less favourable". The WTO Appellate Body declined to take into account the "aims and effects" of a measure under the GATS:

> We see no specific authority either in Article II or in Article XVII of the GATS for the proposition that the "aims and effects" of a measure are in any way relevant in determining whether that measure is inconsistent with those provisions.[128]

Insofar as EU data protection legislation causes "treatment no less favourable" between third countries that are not parties to the EU/EEA, it would be in conflict with the MFN treatment obligation under the GATS. A country's "right to regulate" does not have an impact on the interpretation of GATS Article II that would alter the finding of a GATS violation. Only in a next step may such a GATS violation be justified by invoking as an affirmative defence the right to regulate as emulated in the general exceptions in GATS Article XIV (see Section IV.5.b)).

> Where a measure is inconsistent with the non-discrimination provisions, regulatory aspects or concerns that could potentially justify such a measure are more appropriately addressed in the context of the relevant exceptions. Addressing them in the context of the non-discrimination provisions would upset the existing balance under the GATS.[129]

Risk II
Commission's assessments and decisions on third countries' adequate level of protection *(strong)*
An inconsistent implementation of the adequacy assessment by the Commission could not withstand the tests required under the general exceptions.

Aside from EU legislation on data protection, certain implementation measures have been criticised as susceptible to being found non-compliant with MFN treatment obligation under the GATS. The academic controversy is mainly concerned with the Commission's practice when administering assessments and decisions on third countries' level of adequate protection.[130] The literature in particular notes a different treatment of countries that succeeded in obtaining an adequacy decision incorporating a sectoral scheme for personal data flows from the Commission (such was the invalidated EU-US Safe Harbour) and other third countries.

This argument merits some attention, since the MFN treatment obligation bans both *de jure* and *de facto* discrimination. While it is important that EU data protection law is consistently applied, the legal fallout from a GATS inconsistent refusal to grant a Commission adequacy decision would appear rather confined.[131] This only offers an additional

126 Kristina Irion, "Cloud services made in Europe after Snowden and Schrems", Internet Policy Review, 23 October 2015, available at <http://policyreview.info/articles/news/cloud-services-made-europe-after-snowden-and-schrems/377> (accessed 10 May 2016).
127 Kristina Irion and Giacomo Luchetta, *Online Personal Data Processing and the EU Data Protection Reform* (Brussels: Centre for European Policy Studies, 2013), p. 35f.
128 WTO, Appellate Body Report, *EC – Bananas III* (fn. 104), para. 241.
129 WTO Appellate Body Report, *Argentina – Measures relating to trade in goods and services* (fn. 104), para. 6.115.
130 Perry Keller, *European and International Media Law: Liberal Democracy, Trade and New Media* (Oxford: OUP, 2011), p. 353; Reyes (fn. 103), p. 14f.; Shapiro (fn. 103), p. 71.
131 Without a claimant, obviously there would not be a case (*Nullo actore, nullus iudex*).

argument against fast tracking the adequacy assessment in the context of the US-EU Privacy Shield.[132] Besides, the GDPR will clarify that adequacy decisions by the Commission can concern specified sectors; subject, however, to the same set of elements taken into account during the adequacy assessment (Article 45 GDPR).

c. Domestic regulation

The other GATS obligation on domestic regulation provides:

> In sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner. (GATS Article VI.1)

Under GATS rules on domestic regulation, the DPD can be considered as a measure of general application[133] and falls as such under the requirements of GATS Article VI.1. This provision is primarily about procedural fairness[134] in the administration of such measures, as is clear from its wording. Hence, the DPD itself cannot be challenged under GATS rules on domestic regulation. While – at the level of its application – it is impossible to conclude that there never was and never will be a violation of GATS Article VI.1, this would not affect EU data protection law as such.

The DPD does not trigger paragraphs 2, 3, 4 and 5 of GATS Article VI because it does not mount authorisation, qualification or licensing requirements, nor can it be considered a technical standard.

d. Market access

GATS Article XVI.1 provides for the market access rules:

> With respect to market access through the modes of supply identified in Article I, each Member shall accord services and service suppliers of any other Member treatment no less favourable than that provided for under the terms, limitations and conditions agreed and specified in its Schedule. (GATS Article XVI.1)

There is virtually no risk of violating market access, as the DPD's rules on transfers of personal data to third countries are applied indiscriminately to both domestic and foreign controllers. Next to the rules for ensuring an adequate level of protection in third countries, the derogations in Article 26 DPD provide for standard contractual clauses, ad hoc measures, and a number of conditions in which personal data can be transferred to a third country that does not ensure an adequate level of protection.

GATS Article XVI.2 covers an exhaustive list of six market access barriers, five of which are quantitative restrictions. On their face, DPD rules for the transfer of personal data to third countries are not subject to quantitative restrictions. There is also presently no risk of finding a "zero quota" violating GATS Article XVI.2(a) and (c) due to the derogations in Article 26 DPD for transfers of personal data to third countries that do not ensure an adequate level of protection.[135]

---

132 See e.g. Christopher Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems" University of Cambridge Faculty of Law Research Paper, 14/2016, available at <http://ssrn.com/abstract=2732346> (accessed 8 April 2016).

133 The DPD has a broad territorial scope, horizontally applies to almost all processing of personal data, and defines "personal data" broadly.

134 In the EU, similar administrative procedural rules are derived from the case law of the CJEU.

135 For example, in *US – Gambling* (fn. 104), the WTO Appellate Body interpreted a total prohibition on the remote supply of gambling and betting services as GATS-inconsistent market access limitations. Although per se not a quantitative restriction, the prohibition amounted to a "zero quota" on the number of service suppliers and total number of service operations (GATS Article XVI.2 (a) and (c)), paras. 238, 251, 252.

Even following the CJEU ruling invalidating the EU-US Safe Harbour agreement without temporal restrictions, there has been never a situation in which the EU or a Member State fully suspended the transfer of personal data to the US (see Section II.2.a.iii.)).[136] In fact, the Commission and national data protection authorities offered a grace period for personal data transfers based on the EU-US Safe Harbour framework, and advised resorting to the derogations provided for in Article 26 DPD.[137]

Provided a situation would arise that dictates a full suspension of the rules on transfer of personal data to a certain third country, this could amount to a market access restriction contrary to GATS Article XVI.1 and the finding of a "zero quota" under GATS Article XVI.2(a) and (c). This measure – again not at the level of legislation – would require justification and would therefore be submitted to the general exceptions of GATS Article XIV.

Article 49(1) of the new GDPR includes a ceiling for the transfer of the personal data of a limited number of individuals to third countries in the compelling legitimate interest of an undertaking that is narrowly circumscribed and applies only subsidiarily to alternative legal avenues for such transfer. With a view to its subsidiary nature and the available alternatives, including for transfers subject to appropriate safeguards and derogations for specific situations in Articles 46 and 49 GDPR, this should preclude a violation of the market access commitment under GATS Article XVI.

e. National treatment

GATS Article XVII.1 provides for a specific commitment on national treatment:

> In the sectors inscribed in its Schedule, and subject to any conditions and qualifications set out therein, each Member shall accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of services, treatment no less favourable than that it accords to its own like services and service suppliers.

As a non-discrimination rule, the national treatment commitment covers either formally identical or formally different treatment between like services and service suppliers of a member and its own (GATS Article XVII.2). Following Article XVII.3:

> Formally identical or formally different treatment shall be considered to be less favourable if it modifies the conditions of competition in favour of services or service suppliers of the Member compared to like services or service suppliers of any other Member.

The definition of what constitutes less favourable treatment explicitly covers both formal and actual discrimination.

The DPD applies to domestic and foreign controllers and processors of personal data alike in a non-discriminatory manner and thus, on its face, does not violate national treatment.[138] In practice, however, services and service suppliers in mode of supply 1 (cross-border supply of services) from third countries (outside of the EU/EEA and in the absence of an adequacy decision) are accorded formally identical treatment, which arguably modi-

136 CJEU, case C-362/14 (*Schrems v Data Protection Commissioner*) (fn. 15).

137 Commission, Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), COM(2015) 566 final, 6 November 2015, available at <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf> (accessed 10 May 2016).

138 Gregory Shaffer, "Managing U.S. – EU Trade Relations through Mutual Recognition and Safe Harbour Agreements: "New" and "Global" Approaches to Transatlantic Economic Governance", RSC No. 2002/28 EUI Working Papers, p. 35.

fies the conditions of competition in favour of services or service suppliers based in the EU/EEA.

In order to accrue to a violation of the national treatment specific commitment, the legal assessment proceeds analogue to the test of the MFN treatment obligation. Hence, it needs to be established on a case-by-case basis that it concerns "like" services and services suppliers. Where the differential treatment is not exclusively linked to the origin but to "other factors", a more detailed analysis must be conducted (see Section IV.4.b).

To some extent, EU data protection law already creates "two sets of overlapping requirements with the same purpose that are not co-ordinated with each other".[139] The GDPR will exacerbate the duplication of regulatory requirements for third countries' services and service suppliers. Due to the GDPR's new scope of application (see Section II.2.b.i.), services and service suppliers (operating out of third countries) must genuinely comply with the GDPR when offering goods and services to individuals in the EU. In addition, a fraction of these services and service suppliers have to comply with the rules on transfer of personal data to third countries that do not ensure an adequate level of protection. This could amount to a less favourable treatment than that for domestic services and service providers.

As was explained in relation to the MFN treatment obligation (see Section IV.4.b)), the WTO adjudicating bodies would not take into account the "aims and effects" of measures when appraising whether the difference in treatment that is inherent to the DPD's rules on transfer of personal data to a third country manifest as "treatment no less favourable" compared to domestic services and service suppliers. Insofar as EU data protection law would be in conflict with national treatment commitments, GATS Article V offers economic integration as a ready justification (see Section IV.5.a) below).

5. Justifications

Where a measure is found to violate one or several of the GATS commitments, the agreement provides for a range of justifications and exceptions. By order of their relevance for this study, among others, GATS Article V allows for deeper regional economic integration and GATS Article XIV holds general exceptions for public interest measures.

a. Economic integration

GATS Article V provides for a deviation from GATS obligations and commitments in the situation that members deepen economic integration by way of being a party to or entering into an agreement liberalising trade in services between or among the parties. The EU/EEA internal market forms a regional economic integration in the meaning of GATS Article V, and is notified to the WTO Council for Trade in Services.[140] This provision is capable of justifying an otherwise GATS-inconsistent measure, and would likely be the first line of defence for the EU if an EU measure were found to accord less favourable treatment to a WTO Member State as compared to an EU Member State.

WTO law has to date no precedent in which GATS Article V has been invoked and applied, which is why recourse is taken to the interpretation of the sister provision in GATT Article XXIV.5. The appellate body has interpreted the *chapeau* of GATT Article XXIV.5 ("The provisions of this Agreement shall not prevent…") as requiring that the formation of such an agreement would be prevented if the introduction of the measure concerned would not be allowed.[141]

139 Christopher Kuner, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law", [2015] International Data Privacy Law 5(4), pp. 235-245, p. 244.

140 E.g. WTO Committee on Regional Trade Agreements, Establishment of the European Union, Services (WT/REG39/1 24 April 1998).

141 WTO Appellate Body Report, *Turkey – Textiles* (WT/DS34/AB/R 22 October 1999), para. 58.

The case can be argued that the free flow of personal data within the EU/EEA internal market is contingent on the protection of the right to privacy with respect to the processing of personal data as provided for by the DPD (see Article 2(a)). The GDPR is a full harmonisation that will unify EU Member States' law. A third country outside the EU/EEA, even if treated less favourably than a Member State of the EU/EEA, is unlikely to successfully invoke MFN or national treatment of the GATS.

b. General exceptions

The general exceptions in GATS Article XIV shall effectuate a member's right to regulate, as recognised in the preamble to the GATS. The exception can be invoked to justify a measure violating GATS obligations and commitments. In order to rely on GATS Article XIV, the contested measure needs to meet the material requirements of Article XIV (a) through (e), as well as the provision of the *chapeau*. This section first offers fundamental background on the application of GATS Article XIV before applying it to EU data protection law.

The legal literature notes a significant degree of legal uncertainty and unpredictability as to how WTO adjudicating bodies will apply the general exceptions.[142] That the overall success rate in the reliance on GATS Article XIV has been rather low is not hard currency in debating its merits, although it is certainly an indicator.[143] The facts of the existing case law (GATT and GATS combined) differ vastly: some cases concerned seemingly protectionist measures. The combined case law also cuts across different types of exceptions, with small but potentially significant variations in the attendant legal mechanisms.[144]

Safeguard 8
General exceptions modelled after GATS Article XIV(c)(ii)
(medium)
Subject to certain trade-conforming conditions, the general exceptions provide an affirmative defence to justify otherwise trade-restrictive measure.

To date, there has been no precedent in WTO law that would clarify how the specific exception in GATS Article XIV(c)(ii) would be interpreted and applied in relation to data protection measures. That there is scope for different interpretations can be seen from the variety of different accounts in the literature; these accounts do not converge in their legal assessment and hold a long list of potential issues.[145]

i. Background on GATS Article XIV

Whether a measure, evaluated for its compliance with GATS Article XIV, fulfils the material requirements under Article XIV will depend on the policy objectives pursued by the measure. For this study, the most important test is laid down in paragraph (c)(ii) of this Article, which allows WTO members to adopt and enforce a GATS-inconsistent measure if it is:

142 Reyes (fn. 103), p. 30; Weber (fn. 103), p. 40, more general Burri (fn. 106), p. 3.

143 Looking at the practice of application of GATS Article XIV and analogous Article XX of GATT 1994, Citizen.org argues that these general exceptions are not effective because, as of August 2015, they succeeded only in one out of 44 cases (NB: The count went up to 45 cases). See "Only One of 44 Attempts to Use the GATT Article XX/GATS Article XIV "General Exception" Has Ever Succeeded: Replicating the WTO Exception Construct Will Not Provide for an Effective TPP General Exception", August 2015, available at <www.citizen.org/documents/general-exception.pdf> (accessed 8 April 2016).

144 The WTO case *US – Gambling* (fn. 104) concerning the GATS is a good illustration. The panel clearly stated that it was not decided "that WTO Members do not have a right to regulate, including a right to prohibit, gambling and betting activities."(at para. 7.4.) In this case, the GATS general exceptions of Article XIV(a) were met, but not the *chapeau* because it was not shown that a gambling prohibition in an U.S. statute did not indiscriminately apply to both foreign and domestic service suppliers.

145 Drake and Nikolaides (fn. 103) see a need for clarification; according to Weber (fn. 103), p. 40, the scope of GATS Article XIV(c)(ii) may not except every aspect of data protection laws; Diana A. MacDonald and Christine M. Streatfeild, note many open questions in justifying restrictions of cross-border data flows, "Personal Data Privacy and the WTO" [2014], *Houston Journal of International Law* 36, pp. 625-653; Shin-yi Peng points at the vast deviations in parties' approach to the protection of personal data, "Digitalization of Services, the GATS and the Protection of Personal Data", in *Kommunikation: Festschrift für Rolf H. Weber zum 60. Geburtstag*, p. 753 (Rolf Sethe et al. eds., Schulthess: 2011).

> [N]ecessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to … the protection of the privacy of individuals in relation to the processing and dissemination of personal data….

In relation to GATS Article XIV(c), a WTO appellate body applied a three-tiered test, namely:

1. The measure at issue is designed to "secure compliance" with national laws or regulations;
2. Those national laws and regulations are not inconsistent with the WTO agreement; and
3. The measure at issue is necessary to secure compliance with those national laws and regulations.[146]

These three elements must be demonstrated by the country invoking Article XIV(c), which consequently puts the burden of proof on the respondent.

The core element of the general exceptions is thus a "necessity" test, which requires "weighing and balancing" between several factors.[147] A first step is to evaluate whether a measure contributes to the enforcement of domestic laws and regulations that pursue a public policy interest (this is not to be confused with the contribution of the measure to the protected interest itself) and is "not inconsistent" with the provisions of the GATS.

In a second step, the restrictive effect of the measure on international trade is evaluated. The less restrictive the measure, and the greater the contribution to the enforcement of public interest, the more likely it is that the measure in question will meet the necessity test.[148]

In order to show that the measure does not meet the necessity test, a claimant can demonstrate that a less trade-restrictive alternative to the measure has been "reasonably available". This alternative measure cannot however pose prohibitive costs or substantial technical difficulties to that party.[149]

A measure that has been provisionally justified under the Article XIV(c)(ii) material requirements also has to meet the Article XIV *chapeau*: namely, the measure should have been applied in a manner that does not constitute:

> [...]a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services.

The *chapeau* is interpreted by the WTO adjudicating bodies as an open norm,[150] directed at preventing abuses or misuses of the right to invoke the exception.[151] The benchmark that is often used in order to evaluate the compliance with the *chapeau* is the "consistency of enforcement" of the challenged measure.[152]

---

146 WTO Appellate Body Report, *US – Gambling* (fn. 104), para. 6.536; see also WTO Panel Report, *Argentina – Financial Services* (WT/DS453/R 30 September 2015), paras. 7.655.

147 WTO Appellate Body Report, *US – Gambling* (fn. 104), para. 306; WTO Panel Report, *Argentina – Financial Services,* ibid., para. 7.684.

148 WTO Panel Report, *Argentina – Financial Services* ibid., paras. 7.685, 7.727, referring to WTO Appellate Body Report, *Korea – Various Measures on Beef* (WT/DS161/AB/R and WT/DS169/AB/R 11 December 2000), para. 163.

149 WTO Panel Report, *Argentina – Financial Services*, ibid, para. 7.729 referring to WTO Appellate Body Report, *US – Gambling* (fn. 104), para. 308.

150 The unwillingness of the WTO adjudicating bodies to develop general rules on the basis of the *chapeau* was criticised, as this creates uncertainty in the future interpretation of the exceptions. See Reyes (fn 103), p. 27.

151 WTO, *Argentina – Financial Services - Report of the Panel*, supra, note 49, para. 7.743 referring to WTO, *US – Gasoline- Report of the Appellate Body Report* (WT/DS2/AB/R 29 April 1996).

152 WTO, *US – Gambling - Report of the Appellate Body*, supra, para. 351.

In theory, the *chapeau* of GATS Article XIV formulates a legitimate expectation corresponding to the principles of good regulation that the application of a measure should not discriminate between countries where like conditions prevail.[153] In the interpretation by WTO appellate bodies, the required "consistency" is stricter at the level of legislation and somewhat more lenient when it comes to consistency of enforcement measures.

In the case *US – Gambling*, the Appellate Body confirmed that the US ban on online gambling did not meet the requirement of the GATS Article XIV *chapeau* due to "ambiguity" in relation to the scope of one US statute, which appeared to permit domestic suppliers to have remote betting services for horse racing.[154]

By contrast, isolated instances of enforcement must be placed in their proper context when examining whether a measure's application causes "arbitrary" or "unjustifiable" discrimination. The WTO appellate body in the *US - Gambling* case stated:

> In our view, the proper significance to be attached to isolated instances of enforcement, or lack thereof, cannot be determined in the absence of evidence allowing such instances to be placed in their proper context. Such evidence might include evidence on the overall number of suppliers, and on patterns of enforcement, and on the reasons for particular instances of non-enforcement. Indeed, enforcement agencies may refrain from prosecution in many instances for reasons unrelated to discriminatory intent and without discriminatory effect.[155]

ii. Applying the general exceptions of GATS Article XIV

GATS Article XIV(c)(ii) is specifically about justifying a non-compliant measure that claims to be necessary to secure compliance with – in this case – EU data protection law, which in itself is "not inconsistent" with the GATS. Such a measure can be at the level of implementation of EU data protection law, such as a decision by a competent authority, or a provision from Member States' national data protection law pursuant to the DPD, or (in the near future) a provision from the GDPR.

The identification of the relevant laws or regulations with which the challenged measure secures compliance is of strategic importance for the success of invoking GATS Article XIV(c) as affirmative defence. For example, linking a measure to the rules on transfers of personal data under the DPD, as the relevant laws or regulations would only perpetuate the same legal deficit when it comes to their GATS compliance.

Rather, the relationship between the challenged measure, and the laws and regulations with which said measure secures compliance, should be established with provisions of EU data protection law that do not discriminate between different services and service suppliers.[156] In the event that the differentiation between third countries that ensure an adequate level of protection and those that do not is challenged under the GATS, this measure would secure compliance with elementary principles of EU data protection law.

For the "necessity test", the question is whether the measure is actually "necessary" in order to ensure compliance with the aforementioned laws or regulations, and whether

153 See also the commitment on domestic regulation in GATS Article VI.1 (see Section IV.4.c)); see Weber (fn. 103), p. 35.

154 WTO Appellate Body, *US – Gambling* (fn. 104), para. 369; WTO Panel Report, *US – Gambling* (WT/DS285/R 10 November 2004), para. 6.607.

155 WTO Appellate Body, *US – Gambling*, ibid, para. 356.

156 For example, identifying elementary provisions of EU data protection law, notably the principles relating to data quality (Article 6 DPD), criteria for making data processing legitimate (Article 7 DPD), individual's right of access to data and to object (Articles 12 and 14 DPD), security of processing (Article 17), and available remedies and sanctions (Articles 23 and 24 DPD).

their application is sufficiently consistent in order to not constitute "a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services" in violation of the GATS Article XIV *chapeau*.

The EU rules on personal data transfers to third countries do not create an absolute ban on trade in services (see Section II.2.a).ii. and b).ii.). But even if they are not immensely trade-restrictive, they do have negative effects on international trade in services. For instance, adequacy assessments and compliance with the derogations under Article 26 DPD are costly and time consuming. Overall, a balance has to be struck: firstly, evaluating the importance of the objective in preventing evasion of EU data protection standards; secondly, taking into account the relative contribution of the challenged measures to securing compliance with EU data protection law; and thirdly, considering the negative effect on trade.

Should a dispute arise, it will not be privacy or data protection that will be balanced against trade. Instead, what will be evaluated is the effectiveness of a measure that aims to secure compliance with laws and regulations compared to its relative trade-effectiveness. The required "weighing and balancing" is highly sensitive to the circumstances of the case, and as it is due to the WTO adjudicating bodies' discretion, cannot be fully anticipated.[157]

There are residual legal risks for the EU when relying on GATS Article XIV(c) as an affirmative defence:

First, evidence on the performance of EU data protection law on the one hand, and its discrete impact on international trade in services on the other hand, could influence the "weighing and balancing" required under the "necessity test". A low culture of compliance, for example, as was demonstrated in relation to the now invalidated EU-US Safe Harbour agreement,[158] could undermine the relative strength of a challenged measure's contribution to securing compliance with EU data protection law in view of its trade-restrictive effect.

Second, the "necessity" of the measures needed to secure compliance could eventually be challenged if the complaining party were to invoke less restrictive alternatives capable of securing compliance with data protection laws. By international comparison, EU data protection law promulgates the highest level of formal protections, and these protections are shielded against circumvention via the rules on transfer of personal data to third countries. Putting these rules to a test with other national or regional data protection frameworks could convince WTO adjudicating bodies that there are less restrictive alternatives to securing compliance with EU data protection law.

Third, in a situation where EU data protection law applies to services and service suppliers from third countries (see Sections II.2.a)i. and b)i.), the necessity of the additional rules on transfer of personal data to third countries could be raised (or the other way around). It is true that the derogations available to services and service suppliers from third countries that do not ensure an adequate level of protection result in an additional layer of regulation, which would substantially overlap with other substantive provisions in EU data protection law.

Fourth, even if the provisions on the transfer of personal data to third countries were to be deemed necessary in order to secure compliance with EU data protection law, there

Risk VI

EU measures in relation to the transfer of personal data to third countries not meeting the requirements of "necessity to ensure compliance" and/or the *chapeau* of the general exceptions *(strong)*

There are residual legal risks for the EU when relying on GATS Article XIV(c) as an affirmative defence, which are in parts due to a lack of consistency.

157 See for a mock application of GATS Article XiV(c) to a country's restrictions on cross-border data flows in the financial services sector: MacDonald and Streatfeild (fn. 145), p. 135f.

158 Commission, Communication from the Commission to the European Parliament and the Council on Rebuilding Trust in EU-US Data Flows, COM(2013) 847 final, 27 November 2013, available at <http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf> (accessed 10 May 2016).

is yet an argument that the potentially inconsistent implementation of these provisions[159] will not withstand the test of the *chapeau* of GATS Article XIV. For example, should a violation of the GATS occur in a situation where the EU has denied a third country's application for adequacy assessment or a request to negotiate a sectoral scheme similar to that of the US-EU Privacy Shield, the *chapeau* can hardly be satisfied.[160]

Risk III
Reliance on contractual safeguards and derogations in relation to transfer of personal data to third countries in relation to national security *(strong)*
Personal data transfers can be based on contractual safeguards and derogations, but these facilities cannot protect against third countries' surveillance laws and disclosure authority.

Fifth, considering that following EU law the rules on transfer of personal data third countries extent to a third country's rules on national security and independent supervision further concerns of inconsistency could arise. On the one hand, the contractual safeguards and derogations provided for in EU data protection law do not supersede a third country's national security and disclosure authorities.161 On the other hand, in EU law member states benefit from the internal market in spite of certain member states' own practices to intercept and collect personal data.

6. Consequences and implications

This hypothetical application helps to illustrate how the compliance of EU data protection law would be assessed under the GATS agreement. It demonstrates how GATS obligations and commitments, as well as available justifications, would be applied in a dispute challenging a measure of EU data protection law.

A principle distinction has to be made in whether the measure being challenged for its GATS compliance belongs to EU data protection legislation or Member States' national data protection laws on the one hand, or on the other hand, to implementation measures by the Commission or national data protection authorities.

Through this application it has been possible to refute a number of potential violations of the GATS, for example regarding market access, and to show the important contribution of the GATS justification on economic integration for justifying a third country's potential differential treatment in relation to an EU/EEA Member State.

It has also been possible to identify a conceivable infringement of GATS MFN treatment obligations by EU rules on the transfer of personal data to third countries, as they are found in Chapter IV of the DPD. The derogations available to services and service suppliers of a third country that does not ensure an adequate level of protection could provide weight against a violation. Should a violation be found, the measure would have to pass the admittedly complex test of GATS Article XIV (c) in order for it to be justified.

It must be conceded that the general exceptions in GATS Article XIV can be invoked in order to preserve a WTO member's right to regulate. GATS Article XIV(c) can justify a GATS non-compliant measure that is "necessary to secure compliance with laws or regulations" in relation to "the protection of the privacy of individuals in relation to the processing and dissemination of personal data".

While GATS Article XIV provides for the horizontal justification of a GATS non-compliant measure, its unambiguity as an affirmative defence can reasonably be doubted, in particular with a view to the legal tests that must be performed in order to meet the requirements of "necessary", its circumstantial application, and WTO adjudicating bodies' discretion.

The requirement in GATS Article XIV(c) that the invoked laws or regulations (with which a measure secures compliance) are themselves "not inconsistent" with GATS

159 Reyes (fn. 103), pp. 25, 34.
160 In WTO case *US – Gambling* (fn. 104) the Appellate Body found one inconsistency in US law with the challenged prohibition of remote gambling services, which, as a result, disqualified the measure from being justified under the *chapeau* of GATS Article XIV, para. 369.
161 Kuner (fn 132), p. 15f.

commitments seems inconspicuous in view of substantive provisions of EU data protection law, with which the rules on transfer of personal data to third countries secure compliance.

If the rules on transfer of personal data to a third country of the DPD are the subject of a WTO DSS procedure and the inconsistency with the GATS cannot be justified, the EU would have to repeal or modify the measure in order to comply with the GATS. The GATS-inconsistency of one provision does not render other provisions of the same law or regulation GATS-inconsistent.[162] The legal consequences of a ruling by a WTO adjudicating body are not automatic, but would require EU action.

Moreover, a WTO member that did not succeed in obtaining an adequacy decision by the Commission could make a plausible claim against the EU for infringing GATS MFN treatment and domestic regulation. In the hypothetical event that a WTO adjudicating body finds that the implementation and administration of EU rules on personal data transfers to third countries violates the GATS, and that such a violation cannot be justified under the GATS Article XIV(c)(ii) exception, the consequences are fairly confined to the implementation of EU data protection law.

For example, in order to rectify a violation of the GATS, or to satisfy the necessity test and the *chapeau* of Article XIV(c)(ii), the Commission would have to modify its practice of conducting adequacy assessments of third countries' adequate level of protection.

Unreasonable delay in the implementation of a WTO adjudicating body's decision on the part of the EU does not yield severe practical repercussions. The main aim of the WTO's DSS is the elimination of WTO-inconsistent and trade-restrictive measures, and not punishment of the breaching Member State. Still, retaliation could amount to substantial countermeasures at the discretion of the complaining party.[163]

162 WTO Panel Report, *Argentina – Financial Services* (fn. 147), paras 7.622, 7.625.
163 Van der Bossche and Zdouc (fn. 71), p. 202f.

V. Comparative assessment of international trade and investment law

This section compares the GATS with CETA text and the TTIP and TiSA negotiations in order to identify risks and safeguards for EU standards on privacy and data protection. Our analysis aims to predict how newer international trade and investment agreements, namely CETA, TTIP and TiSA, could influence EU data protection law. This provides the basis for extracting recommendations.

1. The common core of trade in services agreements

International trade agreements follow a certain structure and share a common core, and this aids a comparative analysis. What follows is a brief introduction of the seven core ingredients.

First are commitments on trade in services, which are also referred to as "core disciplines". These include MFN treatment, domestic regulation, market access, and national treatment disciplines. How they are made binding on the parties may differ: for example in the GATS, MFN treatment is automatically binding on the parties whereas market access and national treatment become binding only if and to the extent that the country has indicated in its schedules of commitments.

These commitments can be complemented and expanded in service chapters, for example the GATS Annexes on Financial Services and Telecommunications, among others. Newer trade in services and investment treaties aim to deepen commitment in existing service chapters, as well as to introduce additional service chapters covering so-called "new and enhanced disciplines". CETA, for that matter, holds a chapter on electronic commerce, a sector that is also negotiated in TTIP and TiSA.

Third, international trade and investment treaties often include a right to regulate, which is aimed at preserving a country's ability to keep and introduce new regulations in order to meet national policy objectives. The preamble to the GATS, for instance, underscores members' right to regulate. With newer trade in services and investment treaties, the right to regulate features more prominently in the text, e.g. it is inside the investment chapter in CETA.

Fourth, general exceptions modelled after GATS Article XIV are included in each of the free trade agreements considered here. General exceptions allow countries to adopt trade-restrictive measures in pursuit of other societal interests: subject, however, to certain trade-conforming limitations and conditions. Section IV.5(b) sets out the interpretation and application of GATS Article XIV.

Next, party-specific schedules of commitments are commonly annexed to the free trade agreement. The schedules contain specific commitments on service liberalisation and reservations that can set conditions and exceptions to these commitments.[164] Newer trade and investment treaties endeavour service liberalisation beyond what has been achieved under the GATS (the so-called "GATS-Plus" criteria). The approach to entering commitments and exceptions can take a positive or a negative list technique. The negative list's default is trade liberalisation; however, if properly applied, both techniques can achieve the same degree of market liberalisation or protection.[165]

Sixth, every free trade agreement contains enforcement mechanisms: as a minimum, dispute resolution for the parties to the agreement. The GATS is enforced exclusively through the WTO government-to-government enforcement mechanism, i.e. the DSS. Bilateral free trade agreements have their very own state-to-state dispute resolution mech-

164 See Commission, Services and investment in EU trade deals: Using "positive" and "negative" lists (fn. 111).
165 Ibid.

anisms. Next to state-to-state dispute resolution, newer free trade and investment treaties also feature investor protection via Investor-to-State Dispute Settlement (ISDS), which is more closely examined in Section V.2.f) below.

Last, regulatory co-operation is a means of co-operation between trading partners that newer trade and investment treaties seek to institutionalise. Section V.2.g) discusses regulatory co-operation with the view to influencing regulatory practice in privacy and data protection.

2. Comparison of GATS, CETA, TTIP and TiSA as is

The comparative analysis with which this study has been tasked rests on the comparative overview in Annex 1, covering the texts of the GATS and CETA as well as the TTIP and TiSA negotiation drafts up to May 2016. As previously explained, the overview is structured following the common core of free trade agreements.

At first glance, compared to the GATS, newer free trade and investment treaties are characterised by new and enhanced disciplines and "GATS-Plus" liberalisation ambitions in their schedules of commitments.

The protection of personal data has been contentious in the TTIP and TiSA negotiations.[166] The Commission promised that it will seek to use free trade agreements and TiSA "to set rules for e-commerce and cross-border data flows and tackle new forms of digital protectionism, in full compliance with and without prejudice to the EU's data protection and data privacy rules."[167]

Beyond the WTO regime, the EU's recent free trade agreements – CETA and the still under negotiation TTIP – open new institutional venues where data protection rules could be put on the agenda. These are the so-called "Regulatory co-operation" and "Investment protection" proposals.

a. Commitments/core disciplines

CETA's chapter on cross-border trade in services makes commitments on the cross-border supply and consumption of services, as well as access to auxiliary services. TTIP will also contain a separate chapter on cross-border trade in services. By contrast, TiSA texts reproduce the scope of the GATS regarding the four modes of supply.

Since the core disciplines by and large reproduce existing GATS commitments they are least controversial substance in the negotiations, which are motivated by GATS-Plus commitments on market liberalisation and new and enhanced disciplines. The classical commitments (or "core disciplines") concerning MFN treatment, market access and national treatment are included in CETA and appear in the negotiation texts for the TTIP and TiSA negotiations.

There is a slight change in the formulation of MFN treatment and national treatment in CETA, which departs from "like services and service suppliers" in favour of "in like situations". It is unclear whether this would affect the interpretation of "likeness" by taking circumstances outside of the competitive relationship between services and service suppliers into account. TTIP negotiation texts take a similar direction, whereby the US favours "in like circumstances" instead of the EU proposal "in like situations".

166 European Parliament, The Trade in Services Agreement (TISA): An end to negotiations in sight?, October 2015, p. 22f., available at <http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/570448/EXPO_IDA%282015%29570448_EN.pdf> (accessed 20 May 2016).

167 Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, Trade for All: Towards a more responsible trade and investment policy, COM(2015) 497 final, 14 October 2015, available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0497> (accessed 10 May 2016).

The domestic regulation discipline in CETA does not contain a provision similar to GATS Article VI.1 ("...all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner"). The same holds true for TTIP negotiations. The legal consequences are minimal, as within their scope the other core disciplines would also protect against unreasonable and partial measures by a party to the agreement.

CETA and TTIP depart from holding a general clause on market access commitment as found in GATS Article XVI.1; however, they retain the prohibition of enumerated quantitative restrictions.

b. Service chapters/new and enhanced disciplines

The GATS Annexes on Financial Services and Telecommunications provide examples of the inclusion of rules on specific services at the core of cross-border trade in services, which aim to liberalise and set basic standards. CETA and the prospective TTIP and TiSA agreements aim to enhance market liberalisation in existing service chapters and to include e-commerce as a new discipline.

i. Financial services

The 1994 Understanding on Commitments in Financial Services provides a first example for the combination of a data flow commitment with a carve-out for a member's privacy and data protection legislation.[168] In the banking sector, for example, the requirement to abstain from taking measures preventing the transfer of data by electronic means constitutes a market access obligation. Simultaneously, this provision explicitly provides that:

> Nothing in this paragraph restricts the right of a member to protect personal data, personal privacy, and the confidentiality of individual records and accounts as long as such right is not used to circumvent the provisions of the Agreement.[169]

Safeguard 9
New exceptions in Understanding in Commitments on Financial Services and CETA's Chapter on Financial Services *(strong)*
New prudential carve-outs for data protection laws in connection with new commitments on data flows in the financial services sector.

The EU's proposal for a TiSA Annex on Financial Services reproduces verbatim the carve-out for privacy and data protection regulations in the financial services sector.[170] As a negotiation position, it would be backed by the previously introduced Understanding on Commitments in Financial Services. The provision follows a commitment:

> [...] not to take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, … where such transfers of information, [or] processing of financial information ... are necessary for the conduct of the ordinary business of a financial service supplier.

Chapter Thirteen of CETA on Financial Services takes a different approach to the transfer and processing of information. CETA Article 13.15.1 stipulates a commitment that permits:

> [...] a financial institution or a cross-border financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing if processing is required in the ordinary course of business of the financial institution or the cross-border financial service supplier.

The second paragraph of this Article calls for "adequate safeguards to protect privacy". The subsequent prudential carve-out for the protection of personal information reads:

168 The understanding is not a part of the GATS but an appendix to the Final Act of the Uruguay Round, available at <www.wto.org/english/tratop_e/serv_e/finance_e/finance_e.htm> (accessed 8 April 2016).
169 Ibid., para. 8.
170 EU Proposal for an Annex on Financial Services, Article 14.

> If the transfer of financial information involves personal information, such transfers should be in accordance with the legislation governing the protection of personal information of the territory of the Party where the transfer has originated.

Read in the light of the previous commitment, "transfers" into and out of a party's territory involving personal information is governed by the data protection law in the country of origin of the personal information. In other words, the EU can maintain its rules on the transfer of personal data to a third country in relation to financial services, and there is no dependency with a Commission decision attesting Canada an adequate level of protection in the meaning of Article 25.4 DPD.

The carve-out for the protection of personal information exempts EU data protection law from the scope of Chapter Thirteen of CETA on Financial Services, without any conditions that it must be consistent with other commitments in that Chapter. As a prudential measure, it would have been unnecessary were the general exceptions in CETA, which are modelled after GATS Article XIV, fully sufficient to achieve the same outcome.

The EU's proposal for a TTIP Chapter on Financial Services is similar to its CETA equivalent, including the call for appropriate safeguards for the protection of privacy, among others, in particular with regard to the transfer of personal data. However, it lacks a similar prudential carve-out for the protection of personal information when it is transferred into and out of a party's territory as in CETA.

ii. Electronic communications

The GATS Annex on Telecommunications covers the Access to and use of Public Telecommunications Transport Networks and Services in Article 5. Article 5(c) provides for the use of public telecommunications infrastructure and services for the movement of information within and across borders, and for access to information contained in databases or otherwise stored in machine-readable form in the territory of any party. Article 5(d) contains an exception for security and confidentiality of messages, if such measures are "necessary" and not applied in a manner that would constitute a means of "arbitrary or unjustifiable discrimination or a disguised restriction on trade in services". The exception, which takes recourse to "necessity" and the *chapeau* of the GATS general exceptions in Article XIV, does not extend to measures on the protection of personal data beyond the "security and confidentiality of messages".

The unofficially released TiSA Annex on Telecommunications Services holds a similar provision on Access to and Use of Public Telecommunications in Article 10. The proposals from other negotiating parties, but not the EU, repeat Article 5(c) of the GATS Annex on Telecommunications. The subsequent proposal for an exception adds the protection of the "privacy of personal data of end users of public telecommunications networks or services" next to the "security and confidentiality of messages". The exception is subject to limiting requirements as is in Article 5(d) of the GATS Annex on Telecommunications. Whether a measure is "necessary" would likely be interpreted similar to GATS Article XIV(c).

Certain parties to the negotiations, again not the EU, propose to include a definition of personal information to the TiSA Annex on Telecommunications Services. Including a definition of "personal information", which could contradict definitions in countries' domestic law, is better avoided. So far, exceptions, such as GATS Article XIV, do not have to perform against definitions of "personal information" or "privacy", which remains the party's right to regulate.

Chapter Fifteen of the CETA on Telecommunications, instead of providing for a specific sectoral exception, introduces a positive obligation ("shall") on the parties to take

appropriate measures to protect "security and confidentiality" and "privacy of users" subject to "the requirement that these measures are not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade." (Article 15.3) Instead of "necessary" as in the GATS and TiSA drafts, the measure has to be "appropriate" and consistently applied.

What is unclear is how a positive obligation to regulate in the interest of the "privacy of users" would be operationalised. For example, positive obligation can hardly fit into the GATS' internal logic that a measure in violation of a commitment can be justified.

The EU's proposal for text on services, investment and e-commerce for TTIP does not resemble CETA's Telecommunications Chapter with regards to the protection of the "privacy of users". Privacy and data protection are not mentioned, which does not mean that the Commission is not aiming to protect them while conducting negotiations. The unofficially released Tactical State of Play of the TTIP Negotiations mentions that "progress on these key EU interests might be accelerated if discussions on data flows and computing facilities also advanced faster (allegedly because US telecom operators are very interested in data flows)".[171]

iii. Electronic commerce

Risk VII
Qualitative requirements and/or reference to international standards in relation to new positive obligations to ensure privacy and data protection *(medium)*
New free trade agreements should not define a ceiling to what is an accepted level of protection of personal data which undercuts EU standards.

Electronic commerce is a new discipline for international trade agreements. The CETA text, in Chapter Sixteen on Electronic Commerce, provides for an Article (16.4) dedicated to trust and confidence in electronic commerce. Similar to the CETA Chapter on Telecommunications, it formulates a positive obligation to "adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce." When doing so, parties "shall take into due consideration international standards of data protection of relevant international organisations of which both Parties are a member."

Canada is not signatory to Council of Europe Convention 108, which is open to non-members of Council of Europe. Canada and EU Member States are members of the OECD. In 2013, the OECD Council endorsed a set of Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.[172] Among other aspects, the guidelines set forth a risk regulation approach to restricting transborder data flows, which conflicts with the precautionary approach underlying the rules for transfer of personal data to third countries under the DPD.[173] From the perspective of the EU, any recourse to "international standards of data protection of relevant international organisations", excluding the Council of Europe, does not serve to back EU-style data protection law.[174]

There is no visible progress on privacy and data protection in relation to transatlantic data flows in the TTIP Chapter on Electronic Commerce.[175] Computer services are slated to be part of the TTIP Chapter on Electronic Commerce. Similar to telecommunications, the scoping and definition attempt to isolate the application layer from computing and related services. Nevertheless, data processing, data storage, data hosting and database services can involve personal data, which would call for a qualified exception for the protection of privacy and personal data, including measures on the cross-border transfer of personal data commensurate to EU data protection law.

171 Anon., Note – Tactical State of Play of the TTIP Negotiations (fn. 87), p. 7.
172 OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) (C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79).
173 Ibid., Article 18.
174 See Wolfgang Kilian, International Trade Agreement and European Data Protection Law, [2016], *Computer und Recht international* 2, p. 51-55, p. 54.
175 Commission, TTIP State-of-Play, (fn. 86), p. 4.

TiSA negotiations on an Annex for Electronic Commerce, which has been unofficially released, contain many textual proposals on movement of information that appear to be neither backed nor rejected by EU negotiators. The proposals go as far as to require that no party "may prevent a service supplier of another Party from transferring, [accessing, processing or storing] information, including personal information, within or outside the Party's territory, where such activity is carried out in connection with the conduct of the service supplier's business." Another negotiating party favours basing any movement of information on "informed consent". Hence, the negotiation positions are vastly different, which does not permit robust inferences about their potential impact on EU privacy and data protection standards. Any progress in the TiSA negotiations on an Annex for Electronic Commerce should be closely monitored.

Risk VIII

New commitments on data flows without a unconditional exception for a party's data protection law *(strong)*

This would only raise the bar for justification, and compound pressure on the general exceptions.

An accompanying provision on Personal Information Protection proposes to recognise "the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce." It stipulates positive obligations ("shall") to "adopt or maintain a domestic legal framework that provides for the protection of the personal information of the users of electronic commerce."

Similar to CETA, it invokes the principles and guidelines of international bodies, which are known to differ vastly between the APEC, the OECD and the Council of Europe, for example. In addition, the positive obligation can be difficult to operationalise in a dispute settlement procedure since it would not influence the interpretation of any core discipline, such as MFN treatment.

As part of the Annex for Electronic Commerce, TiSA also endeavours to incorporate computing services. The negotiation text carries a proposal on local infrastructure under which so-called "data localisation" requirements are prohibited. Data localisation concerns domestic requirements mandating the use of computing facilities, computer processing and storage services supplied from within the territory of that country.

On its face, EU data protection law does not require personal data to be processed exclusively via local infrastructure. Nevertheless, the additional layer of rules on transfer of personal data to third countries of the DPP could indirectly encourage data localisation mainly by enterprise customers (see Section IV.4(b)). The present proposal for a prohibition of data localisation in TTiP is not phrased as a non-discrimination rule, and is thus neutral to factual developments induced by a measure on data protection.

iv. The protection of privacy and personal data in new and enhanced disciplines

This overview could illustrate the array of different approaches accounting for individuals' privacy and personal data protection in cross-border settings, ranging from specific exceptions subject to qualitative requirements; prudential carve-outs; and positive obligations to protect taking recourse to unspecified international standards. From the outset, there is a clear advantage to entrusting privacy and personal data to one single coherent system of protection, instead of manoeuvring in a landscape of different sector-specific requirements and standards in addition to the general exceptions.

c. Right to regulate

The GATS preamble recognises member's right "to regulate, and to introduce new regulations, on the supply of services within their territories in order to meet national policy objectives." As was noted by Commissioner Malmström:

> In general, a clause on the right to regulate is a declaration of an important value to all parties to the negotiations and will help a potential dispute settlement panel in interpreting the substantive provisions of an agreement.[176]

Safeguard 10
Stand-alone right to regulate *(weak)*
A right to regulate needs procedural means to be recognised in order to live-up next to the general exceptions.

The only avenue to effectuate the "right to regulate" in relation to a trade-restrictive measure is via the general exceptions subject to certain trade-conforming limitations and conditions. Hence, this right is very much confined to justifying a measure that violates a GATS commitment, which translates into marginal value next to the general exceptions in GATS Article XIV.

The TiSA negotiation text features a very similar provision to the GATS preamble on the right to regulate. Within the CETA texts, the right to regulate only surfaces in the investment chapter. TTIP negotiations converge on the right to regulate as:

> [T]he right to adopt, maintain, and enforce measures necessary to pursue legitimate policy objectives such as protecting society, the environment and public health, consumer protection, ensuring the integrity and stability of the financial system, promoting public security and safety, and promoting and protecting cultural diversity.

It is uncontested that the sectors and interests mentioned are not exclusive but open-ended. Hence, privacy and data protection measures would also fall under the right to regulate, even without an express mention. Similar to positive obligations to protect personal information in the new and enhanced disciplines, reciting sectors and public interests should not obscure that any "right to regulate" would need procedural means to be recognised.

d. General exceptions

The general exceptions in GATS Article XIV are an accepted formula in international trade agreements, and can consequently be found in the CETA text (Article 28.3), in the EU text proposal for services, investment and e-commerce for TTIP, and in the TiSA bracketed drafts (Article I-9). Although CETA does not contain horizontal general exceptions but lists the relevant chapters, this enumeration is comprehensive in relation to trade in services and investment protection.

In relation to privacy and data protection, EU negotiators' textual proposals are identical to GATS Article XIV(c)(ii) (see Section IV.5(b)). As was explained in the previous section, the formula provides for a horizontal exception that is subject to several requirements that have been interpreted in WTO law. Compared to the interests in paragraphs (a) and (b), the threshold of Article XIV(c) is already lower because it applies to measures "necessary to secure compliance with laws or regulations".

EU data protection law, however, could be considered a "barrier to trade" (in relation to the rules on transfer of personal data to third countries) and a "behind the border barrier to trade" (in relation to services and service suppliers to which EU data protection law applies). Justifying a measure under GATS Article XIV(c), which sorts countries into different categories (those that ensure an adequate level of protection and those that do not) and imposes an administrative formality (i.e. the adequacy decision), is – in comparison with "behind the border barriers to trade" – more difficult.

The reason is that such a measure inevitably produces differential treatment between countries and, depending on the evidence and facts, the "weighing and balancing" could tip against the measure's "necessity". Moreover, "necessity" invites views on alternative

176 Answer given by Commission, Ms. Malmström on behalf of the Commission, Parliamentary questions, 5 November 2015, available at <http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2015-012905&language=EN> (accessed 10 May 2016).

options that would secure the compliance with EU data protection law by the third country's services and service suppliers. Incorporating a reference to the principles and guidelines of international bodies could provide a handy argument against EU rules on the transfer of personal data to third countries.

The *chapeau*, on its face, is not an unreasonable requirement, but the way it is applied in WTO law requires almost absolute "consistency" of the legislative framework, which is in practice arguably prone to some failure. The consequence is that any inconsistency risks precluding the justification of a GATS-inconsistent measure. It is for these reasons that "necessary" and the *chapeau* of GATS Article XIV can be challenging and ambiguous.

Alternatives to emulating the general exceptions of GATS Article XIV can be found in newer exceptions on privacy and data protection in new and enhanced disciplines. For example, the formula used in the Understanding on Commitments in Financial Services is straightforward and cuts out the requirement that the measure must be "necessary" to ensure compliance with laws or regulations (see Section V.2.b.i). CETA, in its Chapter on Financial Services, also creates a dedicated exception for the protection of personal information, which clarifies that any cross-border transfer of personal data has to be made in accordance with the data protection law of the country of origin (see Section V.2.b.i).

A solution could be to replace "necessary" to secure compliance with "appropriate" to secure compliance, which is the formulation used in Chapter Fifteen of CETA on Telecommunications. The function of the *chapeau*, while being necessary to prevent arbitrary and unjustified discrimination, should not invite fishing for any "inconsistency", but one that is on par with the trade-restrictive effect of the contested measure before the justification fails. Alternatively, a dedicated exception for cross-border transfers of personal information analogue to the CETA Chapter on Financial Services is advisable.

e. Schedules of commitments

Personal data processing is not recognised as a sector, but is rather inextricably linked to commercial activities and trade in services of all colours.[177] Unlike service sectors, which are contained in the service sector classification list, it would not be possible to use either the negative or positive lists technique to exempt the processing of personal data from international trade agreements.[178] In other words, as opposed to water or audiovisual media or cultural services, it is not possible to enter sectoral limitations to the processing of personal data in the schedule of commitments.

It should also be assumed that schedules of commitments cover, as part of the service classification, the processing of personal data where such activity is carried out in connection with the conduct of the service supplier's business. The EU could consider scheduling horizontal reservations covering every service sector that the processing and the transfer of personal data is subject to its data protection laws. This is of course second best to introducing a robust self-standing exception in the body text of the agreement, but could back the EU's negotiating position as an alternative.

f. Enforcement, in particular investment protection

Today's investment protection furnishes a designated system of arbitration, which allows investors to sue governments for the violation of the rights and protections granted to them under the investment chapters of free trade agreements such as CETA or TTIP. The investors' protection does not however go as far as to require repealing or changing domestic law or measures that have given rise to the violation: investors would "only" be granted financial compensation for their (prospective) losses.[179]

177 See WTO, Services Sector Classification List (MTN.GNS/W/120 10 July 1991); see Weber and Burri (fn. 116), p. 38f.

178 See Commission, Services and investment in EU trade deals, Using "positive" and "negative" lists (fn. 111).

179 Financial compensation is implemented in EU law via Regulation 912/2014 (fn. 65).

Safeguard 11
Investment protection limited to monetary compensation *(medium)*
Investment protection does not require repealing or changing domestic law or measures that have given rise to the violation.

Such investment protection is limited in several ways: by the provisions of "scope", which relates to the definition of "investor" or "covered investment", and substantively by the limited number of claims that the investors can reasonably make. These are: (1) not to be discriminated against; (2) fair and equitable treatment; (3) the safeguard against expropriation; and (4) the right to transfer assets (see below). The preconditions for this protection is that the "violation" on the part of the state concerns "covered investment", and that there is a causal link between the act of the state and the violation of the investors' rights.

In the wake of the recent exponential growth of claims, expansive interpretation of the safeguards by arbitrators, and the magnitude of financial awards,[180] the existing ISDS system has been criticised for privileging investors vis-à-vis broader communities.[181] The concerns with "expropriation" clauses have also given rise to significant criticism concerning arbitration cases where possibly legitimate measures to pursue public policy goals (such as the public health regulation against smoking or the phasing out of nuclear energy) were challenged as "indirect expropriation".

The Commission – as part of its new trade and investment strategy – takes a different approach to investment protection that is more refined in protecting EU's and Member States' right to regulate. This new approach has entered CETA in several ways and shapes the EU's position in TTIP negotations.[182] CETA holds a provision in its investment chapter stating that

1. For the purpose of this Chapter, the Parties reaffirm their right to regulate within their territories to achieve legitimate policy objectives, such as […].
2. For greater certainty, the mere fact that a Party regulates, including through a modification to its laws, in a manner which negatively affects an investment or interferes with an investor's expectations, including its expectations of profits, does not amount to a breach of an obligation under this Section.

Similar to CETA, the EU proposes an "Investors Court" for TTIP, which vests more institutional guarantees commonly associated with regular courts.[183] One of the first legal assessments of the new approach to investment protection concluded that it can preserve the right to regulate, for example in data protection.[184] Ultimately, this study could not accomplish a full assessment of the new investment strategy and investment protection of the Commission, which would require a separate study.

180 UNCTAD, *Recent Issues in IIAS and ISDS* (2015) available at <http://unctad.org/en/PublicationsLibrary/webdiaepcb2015d1_en.pdf> (accessed on 21 May 2016).

181 Peter Muchlinski, Horatia Muir Watt, Gus Van Harten, Harm Schepel, *Statement of Concern about Planned Provisions on Investment Protection and Investor-State Dispute Settlement (ISDS) in the Transatlantic Trade and Investment Partnership (TTIP)*, 2015, available at <https://www.kent.ac.uk/law/isds_treaty_consultation.html> (accessed on 21 May 2016).

182 Commission, "Investment provisions in the EU-Canada free trade agreement (CETA)", February 2016, available at < http://trade.ec.europa.eu/doclib/docs/2013/november/tradoc_151918.pdf> (accessed 15 June 2016); "Joint statement: Canada-EU Comprehensive Economic and Trade Agreement (CETA)", 29 February 2016, available at <http://europa.eu/rapid/press-release_STATEMENT-16-446_en.htm> (accessed on 21 May 2016).

183 Commission, EU proposals for TTIP Chapter II Investment (2015), available at <http://trade.ec.europa.eu/doclib/docs/2015/september/tradoc_153807.pdf> (accessed on 21 May 2016).

184 Stephan Schill, "Auswirkungen der Bestimmungen zum Investitionsschutz und zu den Investor-Staat-Schiedsverfahren im Entwurf des Freihandelsabkommens zwischen der EU und Kanada (CETA) auf den Handlungsspielraum des Gesetzgebers", Study commissioned by German Federal Ministry for Economic Affairs and Energy, 22 September 2014, available at <https://www.bmwi.de/BMWi/Redaktion/PDF/C-D/ceta-gutachten-investitionsschutz,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf)> (accessed 15 June 2016); see for a critique Markus Krajewski, „Anmerkungen …", 24 September 2014, available at <https://www.gruene-bundestag.de/fileadmin/media/gruenebundestag_de/themen_az/EU-USA_Freihandelsabkommen/Thesenpapier_Klageprivilegien_in_CETA.PDF> (accessed 15 June 2016).

g. Regulatory co-operation

Regulatory co-operation aims to enhance ongoing co-operation between trading partners and their regulators, as a means to limit or eliminate old and new "behind the borders barriers to trade" that result from differences in regulation between various countries. Regulatory co-operation aims to create institutional channels for the exchange of information, methodologies and knowledge between regulators in the belief that this mutual engagement will align the ways regulators "think", and consequently act, and thus achieve "bottom up" regulatory convergence.

It is important to underline that regulatory co-operation would not lead to decisions with formal legal/binding power. Its mechanisms are meant to operate on the more subtle level of regulator persuasion, abetted by stakeholders. To the extent that this persuasion is successful however, it will take place in the early stages of the regulatory process, before the legislative process even commences. Since this persuasion operates at the level of the executive, there is a risk that it will, on most occasions, take place largely free of parliamentary oversight and will potentially lack transparency and sufficient possibility for effective civil society participation.

In the following section, the regulatory co-operation institutions and mechanisms of CETA and TTIP are discussed from a comparative perspective.

i. Which institutions will be created?

Both CETA and TTIP envisage three types of regulatory exchanges in regulatory co-operation.[185] First, "bilateral exchange" should take place between regulators or authorities mainly at the central/federal level of government. Since the bilateral exchange in CETA is voluntary, the agreement does not specify this requirement. In contrast, in TTIP, the bilateral exchange at the central level is obligatory, although no particular regulatory outcome has to be achieved. At the non-central level (EU Member States and US states), bilateral exchange is only "encouraged" in cases where proposals threaten to undermine the purpose of TTIP.

Neither CETA nor TTIP thus specifies precisely which institutions should partake in the bilateral exchange. The orientation of the agreements is functional: authorities or regulators whose proposals threaten to undermine the purpose of the agreements may be invited to such a bilateral exchange by the other trade party. In the EU, this should involve authorities that supervise and enforce data protection law (see Section II.3.b), c) and f)).

This of course may give rise to concerns about the impact of bilateral exchange on the relative division of powers among various data protection bodies in the EU at both the national and EU levels. Since bilateral exchange is defined functionally, data protection issues may arise in bilateral exchanges between a broad spectrum of regulators and authorities. This fragmentation may present a risk for the integrated system of data protection in the EU.

The specific issues that should be discussed in bilateral exchange will be brought up either by the trading partner or, indirectly, by stakeholders. Stakeholders, including both the business community and civil society, will be able to raise issues for bilateral exchange through domestic channels (directly with their state or through consultations), or through

185 Compare CETA Chapter 21 Regulatory Co-operation (available at <http://ec.europa.eu/trade/policy/in-focus/ceta/>) and TTIP's Commission Position Paper on Regulatory co-operation from April 2015 (available at <http://ec.europa.eu/trade/policy/in-focus/ttip/documents-and-events/index_en.htm#eu-position> (accessed 21 May 2016) and from March 2016 (<http://trade.ec.europa.eu/doclib/docs/2016/march/tradoc_154377.pdf> (accessed 21 May 2016)). As of 21 May, the latter document is no further displayed on the European Commission's website.

the channels envisaged by the CETA and TTIP (for example joint proposals from stakeholders directed at the main co-ordinating body as described below).

Second, both CETA and TTIP introduce a more institutionalised form of co-operation, with CETA's Regulatory Cooperation Forum and TTIP's Institutional Mechanism.[186] These bodies will have significant agenda setting and implementation powers. In the case of TTIP, the institutional mechanism would prepare an Annual Joint Regulatory Programme that would set up the regulatory co-operation agenda for the upcoming year. Both CETA and TTIP make these bodies responsible for engaging stakeholders, encouraging and facilitating bilateral exchange to identify the possibilities for further co-operation, and more broadly, monitoring the implementation of the agreement.

In terms of the composition of the aforementioned bodies, CETA only states the official ranks of those who will be represented in its Regulatory Cooperation Forum. TTIP discussion papers have been somewhat more specific: the main officials represented more permanently in this body will be trade officials and "regulatory officials",[187] along with the senior officials who will be responsible for specific issues discussed on particular occasions.

Third, several sectoral committees will be created by both CETA and TTIP (such as the sectoral committee on financial services). These sectoral committees will discuss issues that threaten to undermine trade and investment in a particular sector, and will be called upon to identify possibilities for regulatory co-operation, to monitor the implementation in their sectors, and to report to the main co-ordinating body as described above.

Sectoral committees will be composed along the same lines as the institutional mechanism – they should include trade officials, regulatory officials and relevant sectoral experts. If data protection issues are to be discussed in these sectoral committees, this wide range of officials with different disciplinary and institutional backgrounds will be called upon to address them. In the committee for financial services for instance, trade officials, regulatory affairs officials and experts in banking may discuss data protection issues. Neither of the agreements demands the presence of a representative set of experts in these diagonal cases, where for instance data protection is transversely discussed in the sectoral committees.

ii. Comparison between regulatory co-operation in CETA and TTIP

Even after the lowering of the institutional ambition in recent Commission position papers, TTIP's regulatory co-operation is more ambitious than that of CETA for several reasons.

First, the level of obligation undertaken with TTIP would be higher. While CETA is very explicit about regulatory co-operation being voluntary,[188] TTIP strives to make regulatory co-operation obligatory – even if it stipulates that the parties would not be obliged to achieve any particular regulatory outcome.[189] Second, while CETA puts forward a long list of possible modes of co-operation,[190] the Commission's proposal for TTIP's regulatory co-operation chapter is far more specific.

186 Previous versions of the Commission's proposals discussed an ambitious proposal for a "Regulatory co-operation Body". The Commission position papers published in March 2016 (see fn. 150), however, likely in response to the US disinterest in horizontal institutionalised forms of co-operation, refer to a less exacting "institutional mechanism".

187 From the US side, the likely representatives will be the officials from the Office of Information and Regulatory Affairs, while from the EU side, they will be officials from the Commission's Secretariat General, who are responsible for "regulatory analytics" (impact assessments).

188 CETA, Chapter 21, Art. 21.2 para 6.

189 Commission, EU proposal for a TTIP Chapter on Regulatory co-operation, Art. x1 para 4, available at <http://trade.ec.europa.eu/doclib/docs/2015/february/tradoc_153120.pdf> (accessed 10 May 2016).

190 CETA, Chapter 21, Art. 21.4.

A sub-chapter on "good regulatory practices" aims to make the conduct of regulatory impact assessment obligatory, including taking into account TTIP's trade and investment facilitation concerns.[191] Furthermore, it requires the parties to "maintain procedures or mechanisms to promote periodic retrospective evaluations of regulatory frameworks",[192] with potentially far-reaching consequences for the stability of regulatory frameworks. Equally, the regulatory co-operation chapter demands that the parties "maintain internal coordination processes or mechanisms in order to foster good regulatory practices".[193] Third, and most importantly, TTIP aims to grant more formal powers to stakeholders, including extensive rights of participation and the possibility to add issues to TTIP's Regulatory Co-operation Programme.[194]

Risk IX
Regulatory co-operation in relation to producing impact assessments and independent supervision *(weak)*
This may lead to the production of evidence arguing the trade-restrictive effect of EU data protection law and a fragmentation of venue where the regulation is deliberated.

iii. The consequences of regulatory co-operation for data protection

One caveat must be stressed before embarking on the analysis of the impacts. While this analysis is based on the evaluation of the incentives and strategies available to actors, it still remains at some level speculative. Likely, the two agreements would have different impacts on data protection regulation among the trading partners. Higher risk stems from TTIP's regulatory co-operation in which more is to be gained in terms of trade (data flows), but more is also to be lost in terms of protection.

Several factors ground this claim. The two trading partners (the US and Canada) have very different starting positions when it comes to data protection. While Canada is one of the few countries that has been granted an adequacy decision by the Commission, this is not presently the case with the US. Instead, the EU is striving to conclude a special sectoral agreement with the US (the currently discussed Privacy Shield agreement) in order to bridge the gaps in the regulatory approaches between the trading partners.

The main difference between the two approaches is that the US lacks "omnibus" legislation on data protection and safeguards for non-US persons that protect against unfettered state surveillance. It relies on limited legislative intervention in certain sectors, leaving the rest to market mechanisms and self-regulation.[195] The fate of data protection has also been one of the major disagreements between the two trading partners: while the EU does not negotiate the protection of personal data, the US has furthered the inclusion of data flows into the agreement.[196]

CETA's regulatory co-operation is likely to have a lesser impact on data protection rules in the EU since the normative position of the two trading partners largely align. In contrast, TTIP's regulatory co-operation may evolve into a venue for challenging EU data protection law and its implementation. In this case, the state parties do not share normative commitments. In addition, TTIP empowers stakeholders to possibly fuel a process of making data protection regulation the object of regulatory co-operation and eventually renegotiation.

This could be particularly salient in the fields of financial services, electronic commerce, cloud computing and big data. While the new technological developments will require new rules *pro futuro*, the provisions of TTIP leave significant space for interpretation. For

191 Commission, EU Proposal for a TTIP's Chapter on Good Regulatory Practices, Art. 8, available at <http://trade.ec.europa.eu/doclib/docs/2016/march/tradoc_154380.pdf> (accessed 21 May 2016).
192 Ibid., Art. 9. In the EU, the so called "Better Regulation Guidelines" already incorporate such evaluations and "fitness checks".
193 Ibid., Art. 3.
194 Commission, EU proposal for a TTIP Chapter on Regulatory Cooperation, Art. x5 para 2.
195 The Federal Trade Commission can enforce a limited number of data protection issues if they fall under the protection of consumers against unfair and deceptive business practices.
196 On the political debate, see for instance: Jeremy Fleming, "Brussels makes overture on "data flow" agreement in TTIP", Euroactiv 20 March 2015, available at <http://www.euractiv.com/section/trade-society/news/brussels-makes-overture-on-data-flow-agreement-in-ttip/> (accessed 21 May 2016).

instance, the question of what data handling in "the ordinary course of business" means, or will mean, can be interpreted either narrowly or broadly.

The same is valid for provisions on "interoperability". Given that the EU data protection laws (DPD as well as the GDPR) allow for a "contractual" route to the permission of handling private data, regulatory co-operation may become a space for negotiating broader contractual and self-regulation permissions if these are presented as less burdensome for international trade.

iv. Risks and safeguards in regulatory co-operation

By integrating regulatory co-operation into the domestic regulatory processes at the level of the executive, two important procedural safeguards are weakened. First, given that the results of regulatory co-operation do not have the form of "international law", the safeguard mechanisms of the EU legal order discussed above remain inoperative. Second, consigning transatlantic exchange across wide variety of sectors to the exchange among executive officials will further weaken the political control and oversight over the executive branch by political institutions and the general public.

More specifically, the most significant risks presented by regulatory co-operation are:

Fragmentation. The proliferation of various bodies to deal with the issues of data protection in the context of the both TTIP and CETA pose risks to the unified system of EU data protection, including democratic oversight.

Diagonal conflicts. In both CETA and TTIP, both sectoral committees and bilateral exchanges may be called upon to discuss issues of data protection without there being sufficient safeguards that these issues would even be recognised, and, if recognised, whether the representatives dealing with data protection would be called upon to participate in the exchange. This is particularly problematic in the light of EU Charter and EU data protection laws, which give independent supervisory bodies the exclusive authority to oversee the protection of data protection.

Composition. Both, CETA's Regulatory Co-operation Forum and TTIP's Institutional Mechanism, as well as various sectoral committees, will have a prominent representation of trade and regulatory affairs officials. Such a composition will influence the language in which eventual data protection issues will be articulated and justified in the context of regulatory co-operation, which may have consequences for the level of respect afforded to them by these bodies.

Agenda Setting. The stakeholders will have a significant say in the regulatory agenda of TTIP, and to a lesser extent CETA. However, this does not provide the same advantages to all stakeholders. A first obvious reason for this structural disadvantage is that business stakeholders have more resources, which allows them better representation vis-à-vis other stakeholders in the regulatory process.[197]

197 Wendy E. Wagner, "Administrative Law, Filter Failure, and Information Capture", 59 *Duke Law Journal* (2010), pp. 1321-1432; Andrew Baker, "Restraining Regulatory Capture? Anglo-America, crisis politics and trajectories of change in global financial governance",(2000) *International Affairs* 86 (3), pp. 647–663; Maria Green Cowles, "The Transatlantic Business Dialogue" and "Domestic Business-Government Relations" (M. Green Cowles, J. Caporaso, Th. Risse, eds, *Transforming Europe: Europeanization and Domestic Change*, Cornell: Cornell University Press, 2001). Beate Kohler-Koch, "Governing with the European Civil Society", in: (B. Kohler-Koch and Ch. Quittkat, eds., *De-Mystification of Participatory Democracy. EU Governance and Civil Society*, Cambridge: CUP 2013), p. 105.

At the same time, the dominance of trade and regulatory affairs officials in TTIP institutions is likely to be allied with the ideological battle against red tape and barriers to trade, both of which are portrayed as impediments to economic growth. This is, once more, to the advantage of business stakeholders. Stakeholders' proposals aimed at a higher level of data protection, for instance, are likely to be structurally disadvantaged in the context of the free trade agreements.

VI. Conclusion with policy recommendations

The study was tasked with analysing how EU standards on privacy and data protection are safeguarded from liberalisation by existing free trade agreements (the GATS and CETA) and those that are currently being negotiated (TiSA and TTIP). It is imperative to distinguish between safeguards and risks in the EU legal order, on the one hand, and, on the other hand, EU privacy and data protection standards in international trade law.

1. Safeguards and risks in the EU legal order

With the entry into force of the EU Charter of Fundamental Rights, the rights to the protection of privacy and personal data were well entrenched at the level of EU primary law. According to Article 8(2) of the Charter, personal data must be "processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."

The principle of "independent supervision", which is guaranteed by Article 8(3) of the Charter, shields the EDPS, national supervisory authorities and, indirectly, the Article 29 Working Party and the future European Data Protection Board.

The DPD and its successor, the GDPR, provide a comprehensive legal framework that – according to the authoritative interpretation by the Court of Justice – aims to ensure not only effective and complete protection, but also a high level of protection of those fundamental rights and freedoms.

EU data protection law, i.e. today's DPD and tomorrow's GDPR, applies directly to the processing of personal data by cross-border services and service suppliers operating outside of EU territory. In addition, the legislation holds rules on the transfer of personal data outside of the EU/EEA, depending on whether a third country ensures an adequate level of protection or not.

Via the principle of autonomy of the EU legal order, the CJEU guards the supremacy of EU primary law, including Charter rights, vis-à-vis conflicting international law. The advisory opinion procedure in Article 218(11) of the TFEU offers a ready pathway to a CJEU assessment of the compatibility of international trade law with EU law before it takes effect.

International trade law and decisions of dispute settlement bodies have "no direct effect" in EU law. This follows from the EU's recent practice of incorporating a "no direct effect clause" into international trade law, but also from the jurisprudence of the CJEU. In the event that an EU measure would be found inconsistent with international trade law, it would not be automatically invalid or inapplicable, but would require an implementation act from the EU legislator.

The risks for privacy and data protection stemming from the sphere of the EU are, broadly speaking, that EU international relations could place more emphasis on international trade in services relative to EU standards on privacy and data protection. For example, the Commission's assessments and decisions on third countries' adequate level of protection could reasonably be deemed inconsistent, which in turn translates into vulnerability to finding non-compliance with international trade law.

Whereas contractual safeguards and derogations for third countries that do not ensure an adequate level of protection are important safeguards in enabling free trade, they may actually undermine the consistency of adequacy decisions within the regime. This is particularly the case when – in the absence of an adequacy decision – contractual safeguards, such as standards and contractual clauses, are legally viable alternatives for transfers of personal data to a third country. From an EU constitutional perspective, certain member states' and certain third countries' national security can disproportionately restrict the

privacy and data protection rights of individuals, but both cases are treated inconsistently mainly due to EU competencies.

2. Safeguards and risks in WTO law and the GATS

Within the broader field of public international law, WTO law forms an autonomous jurisdiction, which is exclusively enforced through the WTO Dispute Settlement System. The EU and its Member States are original parties to the WTO, and are bound under international law by the WTO agreement, including the GATS.

Measures in relation to EU data protection law can affect trade in services, and hence could be assessed under the GATS. Such a challenge could be directed not only against EU data protection legislation or Member States' national laws implementing EU data protection law, but also against measures implementing and enforcing EU or national data protection law, e.g. adequacy decisions of the Commission.

Most substantive provisions in EU data protection law apply to the processing of personal data by domestic and foreign service suppliers alike in a non-discriminatory manner and thus, on their face, do not violate MFN and national treatment. From the outset, the law does not prohibit or set quantitative restrictions to the cross-border supply of services in such a way that would conflict with market access commitments.

EU rules on the transfer of personal data to third countries, which are intended to protect the EU's high standards on data protection from being circumvented, accord differential treatment to services and service suppliers that process personal data in third countries. This would likely violate MFN treatment unless it can be justified. There is an exception if it can be shown that the legal protection afforded by EU law is already a competitive differentiator between otherwise "like" services and service suppliers.

The general exceptions in GATS Article XIV can be invoked in order to preserve a WTO member's right to regulate. GATS Article XIV(c)(ii) is specifically geared towards justifying a GATS-inconsistent measure that is "necessary to secure compliance with laws or regulations" relating to "the protection of the privacy of individuals in relation to the processing and dissemination of personal data".

As an affirmative defence, the EU would have to demonstrate that its rules on the transfer of personal data to third countries meet the legal tests of GATS Article XIV(c) and its *chapeau*. Whether a WTO appellate body would concur with the legal argument that the measure of the EU or a Member State would meet the "necessary" legal test cannot be anticipated with certainty.

The other requirement of GATS Article XIV(c), according to which the law or regulation with which a measure ensures compliance has to be "not inconsistent" with the GATS, is insofar inconspicuous. After all, the rules on the transfer of personal data to third countries are anti-circumvention measures to safeguard high EU standards on the protection of personal data, and are, in themselves, not inconsistent with the GATS.

The *chapeau* of GATS Article XIV requires that a measure should not be applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or as a disguised restriction on trade in services. Demonstrating the required "consistency of enforcement" could be a challenge for the EU, in particular with a view to administering and adopting adequacy decisions by the Commission.

3. Safeguards and risks in international trade law in the making

International trade law in the making, to which the EU is a negotiation partner, pursues the ambitious agenda to liberalise services beyond what has been achieved under the

GATS ("GATS-Plus"). EU negotiators have no mandate to bargain over EU data protection standards in trade negotiations.

Today, the processing of individuals' personal data is oftentimes inextricably intertwined with the ordinary conduct of business and cross-border trade in services. In particular, EU rules on the transfer of personal data to third countries will continue to risk running into conflict with non-discriminatory treatment in international trade agreements, and this in turn will put pressure on the general exceptions to deliver a justification should a dispute arise.

The lead strategy to safeguarding member countries' privacy and data protection standards is to incorporate general exceptions that are closely modelled on GATS Article XIV. Against the background of GATS Article XIV(c)(ii), however, there is a margin of reasonable doubt as to whether this strategy would suffice to exempt EU data protection standards in any case.

a. Schedules of commitments

It can be assumed that sectors covered by commitments in a party's schedule would almost automatically extend to the processing of personal data where such activity is carried out in connection with the conduct of the service supplier's business. This would also mean that disputes in relation to EU data protection law could arise in almost any sector, and not just in those sectors covered in new and enhanced disciplines.

While there are positive or negative lists techniques to except a commercial sector recognised in the classification system, it would not be possible to except EU data protection law or the processing of personal data in the EU's schedules of commitments in the same way. What remains possible is to introduce a horizontal section in the schedules, or to pedantically enter limitations to each positive list and exceptions to each negative list, in order to exclude the collection, processing and transfer of personal data from specific commitments.

b. A right to regulate?

If it is not actionable, a party's right to regulate is very much confined to measures that are not inconsistent with an international trade agreement, or in case of a trade-restrictive measure, to justify it in the context of the general exceptions. As a minimum, the GATS lets parties define and regulate privacy and data protection, as long as such measures are not inconsistent with the agreement or applied in manner that would constitute a disguised restriction on trade in services.

The new and enhanced disciplines in CETA, TTIP and TiSA inject language covering positive obligations for taking appropriate or adequate measures to protect the privacy of personal information. While such new language underscores a party's right to regulate in this particular area, it is unclear how such positive obligations can be operationalised in a dispute in order to exempt EU measures without recourse to the general exceptions.

What would seem to curtail a party's right to regulate, however, is the introduction of definitions (e.g. "personal information") and any reference to the principles and guidelines of international bodies (e.g. the OECD Guidelines and the APEC Privacy Framework), which as a rule and for the time being undercut EU data protection standards. Any other qualitative benchmark (e.g. "necessary") could impose a ceiling to the intensity and breadth of measures acceptable to attain the public interest objective.

c. Exception for privacy and data protection

Underscoring the formula of the European Parliament, new free trade agreements should best entrust the right to regulate in the field of privacy and data protection to "a compre-

hensive, unambiguous, horizontal, self-standing and legally binding provision". In order to achieve this outcome, the (limited) experience of how GATS Article XIV is interpreted and applied would support a new approach to the exceptions.

The reason why the threshold must be lowered is not only to except EU rules on the transfer of personal data to third countries but moreover other regulatory substance, such as the right to data portability in the GDPR, which is characteristic for EU data protection law but may not be deemed "necessary" to secure compliance with data protection legislation.

The *chapeau*, on its face, is not an unreasonable requirement stemming from international trade law. However, the level of "consistency of enforcement" required could prove difficult to satisfy in practice. Part of this concern is related to the real risk that in spite of omnibus legislation in the EU, some inconsistency prevails at the level of legislation when neatly comparing across sectors. The other concern is the Commission's very own practice of adequacy assessments and decisions, which would likely not perform against a strict standard of consistency. It is for these reasons that meeting the *chapeau* of GATS Article XIV can be challenging.

d. New and enhanced disciplines

CETA and eventually the negotiations on TTIP and TiSA will introduce new and enhanced disciplines, covering the cross-border flow of data in financial services, electronic communications and electronic commerce. It also becomes clear from the texts of the agreements and negotiation drafts that such data would also cover personal data.

Corresponding to the European Parliament's position in its TiSA resolution, additional commitments on the cross-border transfer of information are problematic if this is not bundled together with a prudential and unconditional carve-out that such commitments are entered into subject to the party's privacy and data protection regulations. A good illustration for this technique can be found in Article B.8 of the Understanding on Commitments in Financial Services, which is part of WTO law.

Moreover, in CETA's Chapter on Financial Services, the commitment on data transfer is complemented with an exception for EU rules on the transfer of personal data:

> If the transfer of financial information involves personal information, such transfers should be in accordance with the legislation governing the protection of personal information of the territory of the Party where the transfer has originated.

In the context of CETA, the existence of a Commission decision that attests Canada an adequate level of protection in the meaning of the EU rules on the transfer of personal data should be noted. Hence, this clause is capable of disentangling free trade agreements from the possible existence of an adequacy decision, which is incumbent to EU data protection law.

Since the relevance of this clause is not limited to financial services, similar provisions would consequently be necessary in relation to every commitment on cross-border data flows in new and enhanced disciplines, and probably covering the entire free trade agreement.

Table 1: Overview summarising the findings on safeguards and risks

	EU law	International trade law
Safeguards	1. Charter rights to privacy and data protection ***(strong)*** 2. Independent supervision ***(medium)*** 3. Scope of application of EU data protection law ***(medium)*** 4. Requirement of third countries' adequate level of protection ***(strong)*** 5. Principle of autonomy of EU legal order ***(strong)*** 6. Absence of direct effect ***(strong)*** 7. Advisory opinion procedure provided for in Article 218(11) TFEU ***(strong)***	8. General exceptions modelled after GATS Article XIV(c)(ii) ***(medium)*** 9. New exceptions in Understanding in Commitments on Financial Services and CETA's Chapter on Financial Services ***(strong)*** 10. Stand-alone right to regulate ***(weak)*** 11. Investment protection limited to monetary compensation ***(medium)***
Risks	I. EU international relations emphasise international trade in services ***(medium)*** II. Commission's assessments and decisions on third countries' adequate level of protection ***(strong)*** III. Reliance on contractual safeguards and derogations in relation to transfer of personal data to third countries in relation to national security (***strong***)	IV. Personal data processing is inextricably intertwined with the ordinary conduct of business in most sectors ***(strong)*** V. EU rules on the transfer of personal data to third countries trigger non-discrimination commitments ***(medium)*** VI. EU measures in relation to the transfer of personal data to third countries not meeting the requirements of "necessity to ensure compliance" and/or the *chapeau* of the general exceptions ***(strong)*** VII. Qualitative requirements and/or reference to international standards in relation to new positive obligations to ensure privacy and data protection ***(medium)*** VIII. New commitments on data flows without a prudential carve-out for a party's data protection law ***(strong)*** IX. Regulatory co-operation in relation to producing impact assessments and independent supervision ***(weak)***

4. Conclusions with recommendations

The following recommendations are addressed to EU decision makers and trade negotiators respectively, and list practical steps for how to strengthen and modify existing safeguards on privacy and data protection in order to make them fit for purpose in next generation free trade agreements.

1. Underscoring the formula of the European Parliament, that new free trade agreements should better entrust their right to regulate in the field of privacy and data protection to:

   > … a comprehensive, unambiguous, horizontal, self-standing and legally binding provision based on GATS Article XIV which fully exempts the existing and future EU legal framework for the protection of personal data from the scope of this agreement, without any conditions that it must be consistent with other parts of the [agreement].[198]

2. Underscoring the European Parliament's position that additional commitments concerning free data flows in new and enhanced disciplines should not be disconnected from any reference to the party's privacy and data protection laws. CETA's Chapter on Financial Services, for example, introduces a prudential carve-out for regulating the cross-border transfer of personal data.
3. In relation to new positive obligations that each party shall adopt or maintain a privacy and data protection legal framework, these should not be linked to any qualitative conditions (e.g. "necessary"), nor to the principles and guidelines of international bodies if these would introduce a ceiling for the acceptable level of protection.
4. Pursuant to the EU's current practice, insert "no direct effect" clauses in free trade agreements and Council decisions approving these free trade agreements. In order to forego any finding of "direct effect", avoid reference in EU legal acts to specific provisions in free trade agreements.
5. With a view to protecting EU privacy and data protection standards, it should be incumbent on the European Data Protection Supervisor (EDPS) to issue opinions on the texts of free trade agreements that the EU plans to adopt.
6. When there is reason to believe that a new free trade agreement to which the EU will become a party negatively affects EU privacy and data protection standards, a Member State, the European Parliament, the Council or the Commission should initiate an advisory opinion procedure at the Court of Justice provided for in Article 218(11) of the TFEU.
7. Adequacy assessments and decisions by the Commission must not grant differential treatment to some third countries and not to others. The Commission should adopt procedural rules for the administration of the assessment of adequate level of protection for third countries, thereby facilitating "consistency of enforcement".
8. The Commission should publish impact assessments on preserving the EU's right to regulate in areas of public interest and legal reasoning based on which it concludes, with sufficient certainty, that EU data protection law in all aspects satisfies the requirements of the general exceptions modelled after GATS Article XIV(c)(ii).

198 Resolution of 3 February 2016 containing the European Parliament's recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA), (fn. 1).

9. EU institutions should commission a study into customers' preferences in the outsourcing and provisioning of computer services involving the personal data of customers and employees in order to build an evidence base supporting the fact that EU data protection law is a differentiating factor in the competitive relationship between services and service suppliers.

Annex: Comparative overview of international trade and investment treaties[1,2]

Table of contents

Note 1: EU proposals are blue font. The actual text in the final agreement will be a result of negotiations between the EU and the other party or parties.

Note 2: The confidentiality surrounding TTIP and TiSA trade negotiations certainly take a toll on accessing and analyzing drafts. Also this study had to rely to some extent on unofficially released documents in order to approximate the state-of-play of negotiations.

	GATS[3]	CETA[4]
	Commitments/ disciplines	
		Chapter Nine
		Cross-Border Trade in Services
Most-favoured -nation treatment	***Article II***	***Article 9.5***
	Most-Favoured-Nation Treatment	***Most-favoured-nation treatment***
	1. With respect to any measure covered by this Agreement, each Member shall accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country. 2. A Member may maintain a measure inconsistent with paragraph 1 provided that such a measure is listed in, and meets the conditions of, the Annex on Article II Exemptions. 3. ...	1. Each Party shall accord to service suppliers and services of the other Party treatment no less favourable than that it accords, in like situations, to service suppliers and services of a third country. 2. … 3. …
Domestic Regulation	***Article VI***	***Chapter Twelve***
	Domestic Regulation	***Domestic Regulation***
	1. In sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner. 2. (a) ... (b)... 3. Where authorization is required for the supply of a service on which a specific commitment has been made, the competent authorities of a Member shall, within a reasonable period of time after the submission of an application considered complete under domestic laws and regulations, inform the applicant of the decision concerning the application. At the request of the applicant, the competent authorities of the Member shall provide, without undue delay, information concerning the status of the application. 4. ... 6. ...	{*not relevant*}

TTiP[5]	TiSA[6]
Commitments/ disciplines	
Chapter {X}	
Cross-Border Trade in Services	
Article X.5	***[Article […]:***
Most-Favored Nation Treatment	***Most-Favoured-Nation Treatment***
1. Each Party shall accord to [EU: services and] service suppliers of the other Party [EU: , in respect of all measures affecting the cross-border supply of services,] treatment no less favorable than [US:that] [EU: the treatment] it accords, in like [EU: situations] [US: circumstances], to [EU: services and] service suppliers of [EU: any] [US: a] non-Party. 2. ...	[EU: delete unless there is a parallel economic integration article below] 1. With respect to any measure covered by this Agreement, each Party shall accord immediately and unconditionally to services and service suppliers of any other Party treatment no less favourable than that it accords to like services and service suppliers if any other country. 2. A Party may maintain a measure nconsistent with paragraph 1 provided that such a measure is listed in [AU/CH/EU propose: its [List of [MFN] [JP propose: Article […] Exemptions] [CH propose; AU/EU oppose:, and meets the conditions of the Annex on Article II Exemptions of the GATS].]
Article X.8	***[Article […]:***
Domestic Regulation	***Domestic Regulation]***
{*not relevant*}	2. [US propose; AU/CO/CH/EU/HK/IS/JP/KR/NO/NZ/PE/PK oppose; CA/CL/CR/MX/TR/TW/UY considering: In sectors where specific commitments are undertaken,] Each Party shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner.]

	GATS[3]	CETA[4]
	Commitments/ disciplines	
Market access	***Article XVI***	***Article 9.6***
	Market Access	***Market access***
	1. With respect to market access through the modes of supply identified in Article I, each Member shall accord services and service suppliers of any other Member treatment no less favourable than that provided for under the terms, limitations and conditions agreed and specified in its Schedule. 2. In sectors where market-access commitments are undertaken, the measures which a Member shall not maintain or adopt either on the basis of a regional subdivision or on the basis of its entire territory, unless otherwise specified in its Schedule, are defined as: (a) ... (d) ... {*qantitative limitations}* (e) measures which restrict or require specific types of legal entity or joint venture through which a service supplier may supply a service; and (f) limitations on the participation of foreign capital in terms of maximum percentage limit on foreign shareholding or the total value of individual or aggregate foreign investment.	A Party shall not adopt or maintain, on the basis of its entire territory or on the basis of the territory of a national, provincial, territorial, regional or local level of government, a measure that imposes limitations on: (a) ... (c) ... {*qantitative limitations}*
National treatment	***Article XVII***	***Article 9.3***
	National treatment	***National treatment***
	In the sectors inscribed in its Schedule, and subject to any conditions and qualifications set out therein, each Member shall accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of services, treatment no less favourable than that it accords to its own like services and service suppliers. 2. A Member may meet the requirement of paragraph 1 by according to services and service suppliers of any other Member, either formally identical treatment or formally different treatment to that it accords to its own like services and service suppliers. 3. Formally identical or formally different treatment shall be considered to be less favourable if it modifies the conditions of competition in favour of services or service suppliers of the Member compared to like services or service suppliers of any other Member.	1. Each Party shall accord to service suppliers and services of the other Party treatment no less favourable than that it accords, in like situations, to its own service suppliers and services. 2. …

TTiP[5]	TiSA[6]
Commitments/ disciplines	
Article X.3	***Article I-3***
Market Access	***Market Access***
[EU: In sectors or subsectors where market access commitments are undertaken, neither Party shall] [US: Neither Party may] adopt or maintain [EU: with regards to market access through the crossborder supply of services], either on the basis of [EU: its entire territory or on the basis of a territorial sub-division] [US: a regional subdivision or on the basis of its entire territory], measures that: (a {*qantitative lmitations}*or (b) restrict or require specific types of legal entity or joint venture through which a service supplier may supply a service.]	With respect to market access through the modes of supply identified in Article I-1, each Party shall accord services and service suppliers of any other Party treatment no less favourable than that provided for under the terms, limitations and conditions agreed and specified in its Schedule. 2. In sectors where market-access commitments are undertaken, the measures which a Party shall not maintain or adopt either on the basis of a regional subdivision or on the basis of its entire territory, unless otherwise specified in its Schedule, are defined as: (a).... {*quantiative limitations}*
Article X.4	***Article I-4***
National Treatment	***National Treatment***
1. Each Party shall accord to [EU: services and] service suppliers of the other Party [EU: , in respect of all measures affecting the cross-border supply of services,] treatment no less favorable than [EU: the treatment] [US: that] it accords, in like [EU: situations] [US: circumstances], to its own [EU: services and] service suppliers.] ... [EU: 2. A Party may meet the requirement of paragraph 1 by according to services and service suppliers of the other Party either formally identical treatment or formally different treatment to that which it accords to its own like services and service suppliers. 3. Formally identical or formally different treatment shall be considered to be less favorable if it modifies the conditions of competition in favor of services or service suppliers of the Party compared to like services or service suppliers of the other Party. ...	1. Subject to any conditions and qualifications set out in its Schedule, each Party shall accord to services and service suppliers of any other Party, in respect of all measures affecting the supply of services, treatment no less favourable than that it accords to its own like services and service suppliers. 2. A Party may meet the requirement of paragraph 1 by according to services and service suppliers of any other Party, either formally identical treatment or formally different treatment to that it accords to its own like services and service suppliers. 3. Formally identical or formally different treatment shall be considered to be less favourable if it modifies the conditions of competition in favour of services or service supplier of the Party compared to like services or service suppliers of any other Party.

	GATS[3]	CETA[4]
	Service chapters/ new and enhanced disciplines	
Financial services		
	Understanding on Commitments on Financial Services	***Chapter Thirteen***
		Financial services
		Article 13.15
	Transfers of Information and Processing of Information	***Transfer and processing of information***
	8. No Member shall take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, or that, subject to importation rules consistent with international agreements, prevent transfers of equipment, where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier. Nothing in this paragraph restricts the right of a Member to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of the Agreement.	1. Each Party shall permit a financial institution or a cross-border financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing if processing is required in the ordinary course of business of the financial institution or the cross-border financial service supplier. 2. Each Party shall maintain adequate safeguards to protect privacy, in particular with regard to the transfer of personal information. If the transfer of financial information involves personal information, such transfers should be in accordance with the legislation governing the protection of personal information of the territory of the Party where the transfer has originated.
		Annex 13-A Schedule of the European Union
	The Communities and their Member States undertake commitments on Financial Services in accordance with the provisions of the "Understanding on Commitments in Financial Services" (the Understanding).	7(a): the provision and transfer of financial information, and financial data processing…

TTiP[5]	TiSA[6]
Service chapters/ new and enhanced disciplines	
EU proposal for services, investment and e-commerce text	Trade in Services Agreement Annex [X]: Financial Services, dated 25 September 2015, unofficial release on Wikileaks
Section VI	
Financial Services	
Article 5 - 33	***[EU/PA/US/CA/NO propose: Article X.10:***
Data processing	***[EU/PA/CH/NO propose: Transfers of Information and Processing of Information] [US propose: Transfer of Information]***
1. Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is necessary in the ordinary course of business of such financial service supplier. 2. Each Party shall adopt appropriate safeguards for the protection of privacy and fundamental rights, and freedom of individuals, in particular with regard to the transfer of personal data.	1. [PA/EU/TW/CH/JP/KR/TR/NO/AU/HK/IL/IS/LI/CR propose; NZ considering: [TR propose: subject to any conditions, limitations and qualifications that a Party shall set out in its schedule,] no Party shall take measures that prevent transfers of data by electronic means, into and out of its territory, [CH/EU/IL/NO oppose: for data processing] [CR considering: or that, subject to importation rules consistent with international agreements,] prevent transfers of equipment, where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier. Nothing in this paragraph restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of this Agreement.]
	[US propose: [PE propose: Subject to prior authorization by the regulator,] Each Party shall allow a financial service supplier of another Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the financial service supplier's ordinary course of business. Nothing in this paragraph restricts the right of a Party to adopt or maintain measures to protect personal data, personal privacy and the confidentiality of individual records and accounts, provided that such measures are not used as a means of avoiding a Party's obligations under the provisions of this Article. [PE propose: Each Party shall adopt adequate safeguards for the protections of personal data.]]

	GATS[3]	CETA[4]
	Service chapters/ new and enhanced disciplines	
Electronic communi-cations		
	Annex on Telecommunications	***Chapter Fifteen Telecommunications***
		Article 15.3
	5. Access to and use of Public Telecommunications Transport Networks and Services	***Access to and use of public telecommunications transport networks or services***
	(a) ... (b) ... (c) Each Member shall ensure that service suppliers of any other Member may use public telecommunications transport networks and services for the movement of information within and across borders, ..., and for access to information contained in data bases or otherwise stored in machine-readable form in the territory of any Member. ... (d) Notwithstanding the preceding paragraph, a Member may take such measures as are necessary to ensure the security and confidentiality of messages, subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade in services. (e) ... (f) ... (g) ...	3. Each Party shall ensure that enterprises of the other Party may use public telecommunications transport networks and services for the movement of information in its territory or across its borders, including for intra-corporate communications of these enterprises, and for access to information contained in data bases or otherwise stored in machine-readable form in the territory of either Party. 4. Further to Article 28.3 (General exceptions), and notwithstanding paragraph 3, a Party shall take appropriate measures to protect: (a) the security and confidentiality of public telecommunications transport services; and (b) the privacy of users of public telecommunications transport services, subject to the requirement that these measures are not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade.

TTiP[5]	TiSA[6]
Service chapters/ new and enhanced disciplines	
EU's proposal for services, investment and e-commerce text	TiSA Annex on Telecommunications Services dated April 2015
Chapter [ ]	
Electronic Communications / Telecommunications Text	***Article 10:***
Article 48 Confidentiality of Information	***Access to and Use of Public Telecommunications [CH propose: Transport Networks and] Services***
Each Party shall ensure the confidentiality of electronic communications and related traffic data by means of a public electronic communication network and publicly available electronic communications services without restricting trade in services.	[AU/CL/JP/KR/PE/US propose; NO considering; alt: ... 3. Each Party shall ensure that service suppliers of another Party may use public telecommunications services for the movement of information in its territory or across its borders, including for intra-corporate communications, and for access to information contained in data bases or otherwise stored in machine-readable form in the territory of any Party. 4. Notwithstanding paragraph 3, a Party may take such measures as are necessary to ensure the security and confidentiality of messages, and protect the privacy of personal data of end users of public telecommunications networks or services, provided that such measures are not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or disguised restriction on trade in services.....
	Article 20 ***Definitions***
	[AU/CO/NZ propose: personal information means any information, including data, about an identified or identifiable natural person.]

	GATS[3]	CETA[4]
	Service chapters/ new and enhanced disciplines	
Electronic Commerce		**Chapter Sixteen**
		Electronic Commerce ***Article 16.4*** ***Trust and confidence in electronic commerce*** Each Party should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce and, when doing so, shall take into due consideration international standards of data protection of relevant international organisations of which both Parties are a member.

TTiP[5]	TiSA[6]
Service chapters/ new and enhanced disciplines	
EU proposal for services, investment and e-commerce text:	Trade in Services Agreement (TiSA) Annex on [Electronic Commerce] dated October 2015
Electronic Commerce	***Annex on Electronic Commerce***
	Article 1:
	General Provisions
The provisions on exceptions and the general provisions of this Title including the reference to the right to adopt, maintain and enforce measures necessary to pursue legitimate policy objectives such as consumer protection apply to the entirety of this chapter. (fn 21)	1. [AU/CA/CL/TW/CO/CR/EU/HK/IS/IL/JP/KR/LI/MX/NZ/NO/PA/PE/CH/TR/US propose: This Annex shall apply to measures [CH oppose; IL considering: adopted or maintained] by [CH propose: Parties] [CH oppose: a Party] affecting trade in services [AU/CA/CO/EU/HK/MU/PE/US propose; CL/CR/IL/MX/NO considering: using or enabled] by electronic means.] 2. [CH propose; U/CA/CL/TW/CO/EU/IL/JP/MX/NZ/PE oppose; MU/PK considering: Without prejudice to the policy objectives and legislation of the Parties in areas such as ... the protection of privacy and of the confidentiality of personal and commercial data, ...]
Section III - Computer services	***Article 2***
Article 5-13 Understanding on computer services	***Article 2: [CA/PE/US propose: Movement of Information] [JP/MX/CH propose: Cross-Border Information Flows]***
1. To the extent that trade in computer services is liberalised ..., the Parties shall comply with the following paragraphs. ... 3. Computer and related services, regardless of whether they are delivered via a network, including the Internet, include all services that provide: ... (b) computer programmes defined as the sets of instructions required to make computers work and communicate (in and of themselves), ... (c) data processing, data storage, data hosting or database services; or .... 4. Computer and related services enable the provision of other services (e.g. banking) by both electronic and other means. However, there is an important distinction between the enabling service (e.g. web-hosting or application hosting) and the content or core service that is being delivered electronically (e.g. banking). In such cases, the content or core service is not covered by CPC 84.	X. [CA/CL/CO/MX/NZ/PE propose: The Parties recognize that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.] ... 1. [HK propose: Without prejudice to the domestic legal framework adopted or maintained under Article 4 or for the protection of the privacy of individuals in relation to personal data,] [CA/TW/CO/JP/MX/US propose; PE considering: No Party may prevent a service supplier of another Party from transferring, accessing processing or storing information, including personal information, within or outside the Party's territory, where such activity is carried out in connection with the conduct of the service supplier's business.] ... 4. [CA/CL/CO/JP/MX propose; PE/PK considering: Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 to achieve a legitimate public policy objective, provided that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or disguised a restriction on trade.]

GATS[3]	CETA[4]
Service chapters/ new and enhanced disciplines	

TTiP[5]	TiSA[6]
Service chapters/ new and enhanced disciplines	
	Article 4
	Personal Information Protection
	1. [AU/CA/CL/TW/CO/lL/JP/KR/MX/NZ/ NO/PA/PE/CH propose: The Parties recognize the [CH propose: rights of consumers] [CH oppose: economic and social benefits] of [CH propose: the protection of] [CH oppose: protecting] the personal information [CH oppose: of users of electronic commerce] and the contribution that this makes to enhancing consumer confidence in electronic commerce.] 2. [AU/CA/CL/TW/CO/IL/KR/MX/NZ/ NO/PA/PE/CH propose: [CH oppose: To this end,] each Party shall adopt or maintain a domestic legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of these personal information protection frameworks, each Party should take into account principles and guidelines of relevant international bodies.] [CA propose: Each Party shall ensure that its domestic legal framework for the protection of personal information of users of electronic commerce is applied on a non-discriminatory basis.] 3. [AU/CA/CL/TW/CO/IL/JP/KR/MX/NZ/ NO/PA/PE/CH propose: Each Party [CH propose: shall] [CH oppose: should] publish [CH propose: comprehensive] information on the personal information protections it provides to users of electronic commerce, including: (a) how individuals can pursue remedies; and (b) how business can comply with any legal requirements.]

GATS[3]	CETA[4]
Service chapters/ new and enhanced disciplines	

TTiP[5]	TiSA[6]
Service chapters/ new and enhanced disciplines	
	Article 8
	Article 8: Location of Computing Facilities [KR propose:1]
	X. [CA/CL/PE propose: The Parties recognize that each Party may have its own regulatory requirements regarding the use of computing facilities including requirements that seek to ensure the security and confidentiality of communications.] 1. [CA/CO/JP/PE/PK/US propose; CH oppose; MX considering: No Party may require a service supplier, as a condition for supplying a service [CO oppose: or investing in its territory], to use or locate computing facilities in the Party's territory.] 2. [CH propose; KR oppose: Parties should not require suppliers of electronic commerce to use or establish any local infrastructure as a condition for the supply of services.] 3. [CA/CL/CO/JP/MX/PK propose: Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 to achieve a legitimate public policy objective, provided that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or disguised a restriction on trade.] ...
	Article 14: Definitions
	For purposes of this Annex: ... [AU/CA/CO/NZ propose: personal information means any information, including data, about an identified or identifiable natural person;] [Proponents will consult on this definition of personal information.] …

	GATS[3]	CETA[4]
	Right to regulate	
Right to regulate	***Preamble***	
	Recognizing the right of Members to regulate, and to introduce new regulations, on the supply of services within their territories in order to meet national policy objectives and, ...	

TTiP[5]	TiSA[6]
Right to regulate	
[EU: Article X-2	*[Article […]:*
Scope [US: and Coverage]	***Domestic Regulation]***
The Parties, ..., hereby lay down the necessary arrangements for the progressive reciprocal liberalization oftrade in services, for the liberalization of investment, and for facilitation of e-commerce. Consistent with the provisions of this Title, each Party retains the right to adopt, maintain, and enforce measures necessary to pursue legitimate policy objectives such as protecting society, the environment and public health, consumer protection, ensuring the integrity and stability of the financial system, promoting public security and safety, and promoting and protecting cultural diversity.]	1. Parties recognize the right to regulate, and to introduce new regulations, on the supply of services within their territories in order to meet [AU/CA/CL/CO/EU/IS/KR/ MX/NO/NZ/PE/TW/US propose; HK/JP considering: their] [AU/CA/CR/EU/ IS/LI/MX/NO/TR/TW ropose: public] [CH propose: national] policy objectives.
EU's proposal for services, investment and e-commerce text:	
Article 1-1	
Objective, coverage and definitions	
cf. above.	

	GATS[3]	CETA[4]
	General exceptions	
General exceptions		
	Article XIV	***Article 28.3***
	General Exceptions	***General exceptions***
	Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures: ... (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: ... (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; ...	2. For the purposes of Chapters Nine (Cross-Border Trade in Services), ..., Twelve (Domestic Regulations), Thirteen (Financial Services), ..., Fifteen (Telecommunications), Sixteen (Electronic Commerce), and Sections B (Establishment of investments) and C (Nondiscriminatory treatment) of Chapter Eight (Investment), subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by a Party of measures necessary: ... (c) to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: ... (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; ....

TTiP[5]	TiSA[6]
General exceptions	
EU's proposal for services, investment and e-commerce text:	
Chapter VII - General Exceptions ***Article 7 - 1*** ***General exceptions***	***Article I-9:*** ***General Exceptions***
Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on establishment of enterprises, the operation of investments or cross-border supply of services, nothing in Chapter II Section 1, Chapter III, Chapter IV, Chapter V and Chapter VI shall be construed to prevent the adoption or enforcement by any Party of measures: (e) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Title including those relating to: ... (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; ...	Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Party of measures: ... (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: ... (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; ...

	GATS[3]	CETA[4]
	Schedules of commitments	
Schedules	EU Schedule of Specific Commitments {see Note 1}	ANNEX I Schedule of the European Union Reservations applicable in the European Union (applicable in all Member States of the EU unless otherwise indicated)
	{Note: EU's limitations do not concern processing of personal data.}	*{Note: EU's limitations do not concern processing of personal data.}*

TTiP[5]	TiSA[6]
Schedules of commitments	
EU services and investment offer made in the context of Transatlantic Trade and Investment Partnership negotiations	EU initial offer dated September 2013
{Note: EU's limitations and reservations do not concern processing of personal data.}	*{Note: EU's limitations and reservations do not concern processing of personal data}*

	GATS[3]	CETA[4]
	Dispute settlement	
State-to-state	***Article XXIII***	***Chapter Twenty-Nine***
	Dispute Settlement and Enforcement	***Dispute Settlement***
		And as modified by service chapters on Financial services, Telecommunications. Electronic commerce
Investor protection		***Chapter Eight***
		Investment
		Article 8.1 Definitions
		For the purposes of this Chapter: … covered investment means, with respect to a Party, an investment: (a) in its territory; (b) made in accordance with the applicable law at the time the investment is made; (c) directly or indirectly owned or controlled by an investor of the other Party; and (d) existing on the date of entry into force of this Agreement, or made or acquired thereafter; ...
		investment means every kind of asset that an investor owns or controls, directly or indirectly, that has the characteristics of an investment, which includes a certain duration and other characteristics such as the commitment of capital or other resources, the expectation of gain or profit, or the assumption of risk. Forms that an investment may take include: ...
		Article 8.9
		Investment and regulatory measures
		1. For the purpose of this Chapter, the Parties reaffirm their right to regulate within their territories to achieve legitimate policy objectives, such as the protection of public health, safety, the environment or public morals, social or consumer protection or the promotion and protection of cultural diversity. 2. For greater certainty, the mere fact that a Party regulates, including through a modification to its laws, in a manner which negatively affects an investment or interferes with an investor's expectations, including its expectations of profits, does not amount to a breach of an obligation under this Section. ...

TTiP[5]	TiSA[6]
Dispute settlement	
Chapter [ ]	**PART IV**
Dispute Settlement	**Institutional Provisions**
{place holder}	**Section 1: Resolution of disputes**
	{place holder}
EU proposal for Investment Protection and Resolution of Investment Disputes	
Chapter II - Investment	
Definitions specific to investment protection	
'covered investment' means an investment which is owned, directly or indirectly, or controlled, directly or indirectly, by investors of one Party in the territory of the other Party made in accordance with applicable laws, whether made before or after the entry into force of this Agreement.	
'investment' means every kind of asset which has the characteristics of an investment, which includes a certain duration and other characteristics such as the commitment of capital or other resources, the expectation of gain or profit, or the assumption of risk. Forms that an investment may take include: ...	
Article 2	
Investment and regulatory measures/ objectives	
1. The provisions of this section shall not affect the right of the Parties to regulate within their territories through measures necessary to achieve legitimate policy objectives, such as the protection of public health, safety, environment or public morals, social or consumer protection or promotion and protection of cultural diversity. 2. For greater certainty, the provisions of this section shall not be interpreted as a commitment from a Party that it will not change the legal and regulatory framework, including in a manner that may negatively affect the operation of covered investments or the investor's expectations of profits. ...	

GATS[3]	CETA[4]
Dispute settlement	
	Resolution of investment disputes between investors and states (Articles 8.18 ff.)
	Article 8.31 ***Applicable law and interpretation***
	2. The Tribunal shall not have jurisdiction to determine the legality of a measure, alleged to constitute a breach of this Agreement, under the domestic law of the disputing Party. For greater certainty, in determining the consistency of a measure with this Agreement, the Tribunal may consider, as appropriate, the domestic law of the disputing Party as a matter of fact. In doing so, the Tribunal shall follow the prevailing interpretation given to the domestic law by the courts or authorities of that Party and any meaning given to domestic law by the Tribunal shall not be binding upon the courts or the authorities of that Party.

TTiP[5]	TiSA[6]
Dispute settlement	
Section 3 - Resolution of Investment Disputes and Investment Court System	
Article 13 Applicable law and rules of interpretation	
3. For greater certainty, pursuant to paragraph 1, the domestic law of the Parties shall not be part of the applicable law. Where the Tribunal is required to ascertain the meaning of a provision of the domestic law of one of the Parties as a matter of fact, it shall follow the prevailing interpretation of that provision made by the courts or authorities of that Party. 4. For greater certainty, the meaning given to the relevant domestic law made by the Tribunal shall not be binding upon the courts or the authorities of either Party. The Tribunal shall not have jurisdiction to determine the legality of a measure, alleged to constitute a breach of this Agreement, under the domestic law of the disputing Party.	

	GATS[3]	CETA[4]
	Regulatory cooperation	
Regulatory Cooperation		**Chapter Twenty-one**
		Regulatory Cooperation
		Article 21.3 Objectives of regulatory cooperation
		The objectives of regulatory cooperation include to: … (b) build trust, deepen mutual understanding of regulatory governance and obtain from each other the benefit of expertise and perspectives in order to: (i) improve the planning and development of regulatory proposals; (ii) promote transparency and predictability in the development and establishment of regulations; (iii) enhance the efficacy of regulations; (iv) identify alternative instruments; (v) recognise the associated impacts of regulations; (vi) avoid unnecessary regulatory differences; and (vii) improve regulatory implementation and compliance; ...
		Article 21.6 ***The Regulatory Cooperation Forum***
		A Regulatory Cooperation Forum ("RCF") is established, pursuant to Article 26.2.1(h) (Specialised committees), to facilitate and promote regulatory cooperation between the Parties in accordance with this Chapter. …
		Article 21.8 ***Consultations with private entities***
		In order to gain non-governmental perspectives on matters that relate to the implementation of this Chapter, each Party or the Parties may consult, as appropriate, with stakeholders and interested parties, including representatives from academia, think-tanks, non-governmental organisations, businesses, consumer and other organisations. These consultations may be conducted by any means the Party or Parties deem appropriate.

TTiP[5]	TiSA[6]
Regulatory cooperation	
Initial Provisions for CHAPTER [ ]	
[EU: Regulatory Cooperation][US: Regulatory Coherence …]	
[Article X.1:] [EU: General Objectives and Principles	
1. The general objectives of this Chapter are: (a) To reinforce regulatory cooperation thereby facilitating trade and investment in a way that supports the Parties' efforts to stimulate growth and jobs, while pursuing a high level of protection of, inter alia, … personal data … 2. The provisions of this Chapter do not restrict the right of each Party to maintain, adopt and apply measures to achieve legitimate public policy objectives, such as those mentioned in paragraph 1, at the level of protection that it considers appropriate, in accordance with its regulatory framework and principles.	
[Article X.18:] [EU: Bilateral Cooperation Mechanism	
1. The Parties hereby establish a bilateral mechanism to support regulatory cooperation between their regulators and competent authorities at central level to foster information exchange and to seek increased compatibility between their respective regulatory frameworks, where appropriate. 2. The mechanism would further aim at identifying priority areas for regulatory cooperation to be reflected in the Annual Regulatory Cooperation Program ... 3. ...	
[Article X.23:] [EU: Establishment of the Regulatory Cooperation Body	
1. The Parties hereby establish a Regulatory Cooperation Body (hereafter "RCB") in order to monitor and facilitate the implementation of the provisions set out in this Chapter and ... of this Agreement.	

GATS[3]	CETA[4]
Regulatory cooperation	

TTiP[5]	TiSA[6]
Regulatory cooperation	
[Article X.24:] [EU: Participation of Stakeholders	
1. The RCB shall hold, at least once a year, a meeting open to the participation of stakeholders to exchange views on the Annual Regulatory Cooperation Program …	
[Article 25:] [EU: Composition and Rules of Procedures	
1. The RCB shall be composed of representatives of both Parties. It shall be co-chaired by senior representatives of regulators and competent authorities, regulatory coordinating activities and international trade matters. …	

Note 3: General Agreement on Trade in Services (GATS), Annex 1B to the Agreement Establishing the World Trade Organization, Appendix to the Final Act of the Uruguay Round, available at <https://www.wto.org/english/docs_e/legal_e/26-gats.pdf> (accessed 10 May 2016); Understanding on Commitments on Financial Services, Appendix to the Final Act of the Uruguay Round, available at <www.wto.org/english/tratop_e/serv_e/finance_e/finance_e.htm> (accessed 10 May 2016); EU Schedule of Specific Commitments (GATS/SC/31 of 15 April 1994), Supplement 1 (GATS/SC/31/Suppl.1 of 28 July 1995), Supplement 2 (GATS/SC/31/Suppl.2 of 28 July 1995), Supplement 1 Revision (GATS/SC/31/Suppl.1/Rev.1 of 4 October 1995); Supplement 3 (GATS/SC/31/Suppl.3 of 11 April 1997), Supplement 4 (GATS/SC/31/Suppl.4 of 26 February 1998), Supplement 4 Revision (GATS/SC/31/Suppl.4/Rev.1 of 18 November 1999); Unofficially Consolidated GATS Schedule (EU-25) dated 9 October 2006, available at <http://trade.ec.europa.eu/doclib/docs/2008/september/tradoc_140355.pdf> (accessed 10 May 2015).

Note 4: Comprehensive Economic and Trade Agreement (CETA), Official text after legal review, available at <http://trade.ec.europa.eu/doclib/docs/2016/february/tradoc_154329.pdf> (accessed 10 May 2015).

Note 5: Transatlantic Trade and Investment Partnership (TTIP), Unofficial release dated 30 November 2015, Greenpeace TTIP Leaks, available at <https://www.ttip-leaks.org/> (accessed 10 May 2016); Commission, The Transatlantic Trade and Investment Partnership (TTIP) – State of Play, 27 April 2016, available at <http://trade.ec.europa.eu/doclib/docs/2016/april/tradoc_154477.pdf> (accessed 10 May 2016); EU proposal for services, investment and e-commerce text, made public on 31 July 2015, available at <http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153669.pdf> (accessed 10 May 2016); EU proposal for Investment Protection and Resolution of Investment Disputes, made public on 12 November 2015, available at <http://trade.ec.europa.eu/doclib/docs/2015/november/tradoc_153955.pdf> (accessed 10 May 2016); EU initial proposal for legal text on "Dispute Settlement (Government to Government)" in TTIP, made public on 7 January 2015; available at <http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_153032.pdf> (accessed 10 May 2016). EU proposal for legal text on "Regulatory Cooperation" in TTIP, made public on 21 March 2016, available at <http://trade.ec.europa.eu/doclib/docs/2016/march/tradoc_154377.pdf> (accessed 10 May 2016). The actual text in the final agreement will be a result of negotiations between the EU and US.

Note 6: Trade in Services Agreement (TiSA), TiSA core text dated 24 April 2015, unofficial release on Wikileaks, available at <https://wikileaks.org/tisa/core/TiSA-Core-Text.pdf> (accessed 10 May 2016); Trade in Services Agreement Annex [X]: Financial Services, dated 25 September 2015, unofficial release on Wikileaks, available at <https://wikileaks.org/tisa/document/20150925_Annex-on-Financial-Services/20150925_Annex-on-Financial-Services.pdf> (accessed 1 July 2016); EU proposal in the context of the "Trade in Services Agreement – TiSA" for Core Text provisions, March 2013, available at <http://trade.ec.europa.eu/doclib/docs/2014/july/tradoc_152687.pdf> (accessed 10 May 2016); EU proposal for a TiSA Section on "Financial Services", July 2013, available at <http://trade.ec.europa.eu/doclib/docs/2014/july/tradoc_152688.pdf> (accessed 10 May 2016); TiSA Annex on Telecommunications Services dated April 2015, unofficial release on Wikileaks, available at <https://wikileaks.org/tisa/telecommunication/04-2015/TiSA-Annex-on-Telecommunication-Services.pdf> (accessed 10 May 2016); TiSA Annex on Electronic Commerce dated October 2015, unofficial release on Wikileaks, available at < https://wikileaks.org/tisa/document/20151001_Annex-on-Electronic-Commerce/20151001_Annex-on-Electronic-Commerce.pdf> (accessed 1 July 2016). The actual text in the final agreement will be a result of negotiations between the EU and the other parties.