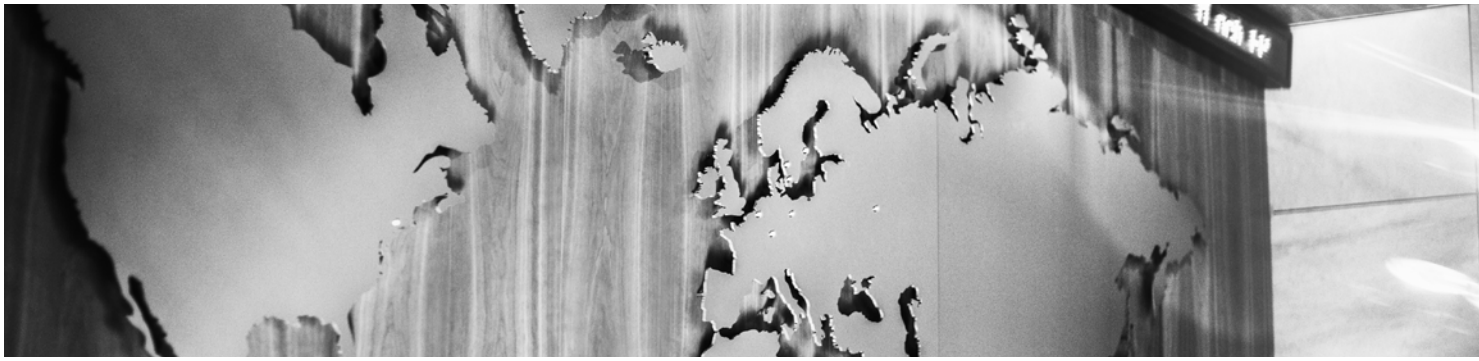
A REPORT BY
MANNHEIMER SWARTLING

19 OCTOBER 2016

Data flows

– Allowing free trade agreements to strengthen the GDPR



CONTACTS

Erica Wiking Häger
Partner and Head of Corporate Sustainability and Risk Management, specialised in data protection and privacy
+46 8 595 063 30
erica.wiking.hager@msa.se

Carolina Dackö
Specialist Counsel, specialised in international trade law
+46 31 355 17 48
carolina.dacko@msa.se

MANNHEIMERSWARTLING.SE

This report provides a legal analysis of two potentially conflicting fields of interest; cross-border data flows and protection of personal data, and how they both would be served by being addressed and balanced in the Transatlantic Trade and Investment Partnership ("TTIP").

The report starts from the premise that data flows, at present, do not benefit from any internationally agreed trade rules that ensure predictability or free cross-border movement. It then turns to a brief analysis of the underlying reasoning behind the EU's rules on protecting personal data, which prohibits or restricts cross-border data flows, when they contain personal data. Next, the report highlights why these rules would be vulnerable if challenged at the WTO. It concludes that, in the interest of preserving these rules, the EU should negotiate provisions allowing data flows in a bilateral or multilateral context, preferably the TTIP.

MANNHEIMER SWARTLING

Introduction

Cross-border data flows have become a fundamental part of many international companies' daily operations. As with trade flows of physical products, when data crosses borders it can be subject to the laws of several jurisdictions, such as those governing the place where the data is originally collected, where it is stored, and where it is processed. While multilaterally-agreed trade rules ensure a certain level of predictability for trading in goods (GATT)[1] and services (GATS)[2], **there are little to no multilaterally-agreed trade rules to ensure such predictability for cross-border data flows**.

In the absence of such rules, legislators in each jurisdiction are free to adopt *domestic* laws that – either intentionally or unintentionally – restrict cross-border data flows to or from other countries. Governments may introduce such restrictions for a variety of reasons, such as the protection of personal data or national security.

The same governments often negotiate broad free trade agreements with other countries in order to open markets and encourage the free flow of goods and services, as well as to agree on fixed and predictable trading rules. To achieve a functioning open market through such agreements, stakeholders have argued for the inclusion of legally binding provisions that ensure predictability for the (free) movement of data flows.

In the following, we give brief analysis of the EU General Data Protection Regulation[3] (the "**GDPR**"), which is a so-called *domestic regulation* under international trade law.[4] Thereafter, we look at the risk that the GDPR would face if reviewed under the WTO rules, especially under GATS Art. XIV. We also analyse a possible rationale for the EU to negotiate a common position on data flows with the US in the TTIP, a broad free trade agreement, **to help shift the balance in favour of the GDPR if ever challenged under international trade law rules**.

1 The General Agreement in Tariffs and Trade 1994.
2 The General Agreement in Trade in Services.

3 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 processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. L 119/1, 4.5.2016.
4 While the GDPR is a legal instrument passed at the EU level, international trade law (e.g. WTO) uses the term "domestic regulations" to refer to rules and laws applied within the national jurisdiction of a WTO member. For the purpose of this report, therefore, EU legislation such as the GDPR is referred to as a domestic regulation or law.

The GDPR and the regulation of data flows

Reconciliation of data protection and free movement of personal data in the GDPR

The EU will soon transition from the currently applicable Directive 95/46/EC, to the GDPR, which reinforces the EU rules on data protection for the internal market. The GDPR will start to apply on 25 May 2018, and will **reaffirm the EU's stance that cross-border data transfers containing personal data are forbidden, unless expressly permitted under any of the specific exceptions**.[5] This approach stands in stark contrast to the US legal framework, which permits data transfers unless otherwise prohibited or restricted for a specific reason.

The GDPR reconciles the conflict between two opposing fundamental EU legal principles: the consistent and comprehensive **protection of personal data** through the EU on the one hand (Art. 1(2)), and the **free movement of such personal data within the internal market** on the other (Art.1(3)).[6] The EU legislator has weighed these principles against each other, and ultimately struck a balance between them in order to ensure that as far as possible, both are respected on the internal market. **In the section below, we review how the EU legislator justified its decision. Thereafter, we review how this reasoning is extended to cross-border data transfers through the GDPR's extraterritorial application. Corresponding reasoning, i.e. the balancing of fundamental principles, could, arguably, be transposed to the EU's negotiating position in the TTIP.**

Protection of personal data in the Charter of Fundamental Rights of the EU

The Charter of Fundamental Rights of the EU (the "**Charter**") embeds the rights of the European Convention of Human Rights into the EU's legal framework.[7] The Charter is *primary* EU law, which means that provisions therein prevail in the case of a conflict with any other EU legal acts adopted by the EU institutions.

Article 8(1) of the Charter sets down the right to the protection of personal data. Article 8(2) regulates under what conditions such data may be processed: (i) for specific purposes, (ii) under consent or "*other legitimate basis laid down by law*" and (iii) that anyone has the right to access data that has been collected and a right to have it rectified.[8] Article 8(3) states that these rules must be subject to control by an independent authority.

Whilst establishing the right to the protection of personal data, **the Charter's provisions clearly acknowledge that the right is not absolute**. Rather, it sets out the conditions under which the processing of personal data should be allowed.

Free movement of personal data within the EU guaranteed by the GDPR

The preamble of the GDPR explains that while the right to protection of personal data is enshrined in the Charter, other fundamental rights may infringe on that right (recital 4):

> "The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."[9] [emphasis added]

Furthermore, the legislator has chosen to adopt the new data protection regime in the form of a regulation, in order to "*prevent divergences hampering the free movement of personal data within the internal market*."[10]

5 See Art. 44 of the GDPR.

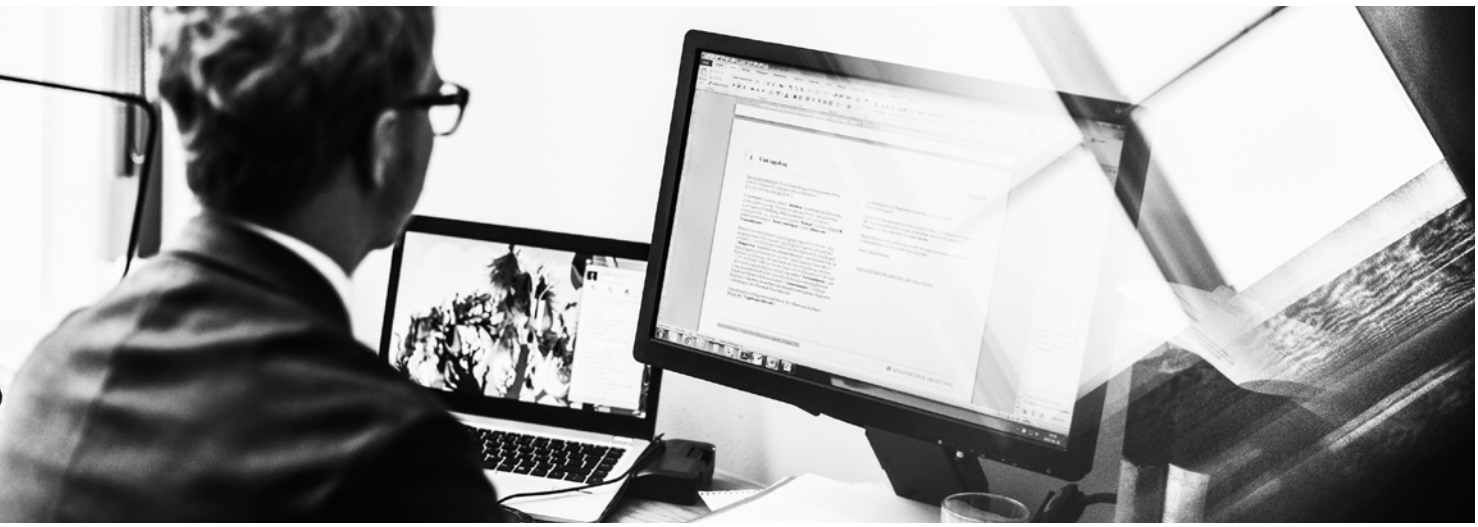
6 See also Art. 16(2) of the Treaty on the Functioning of the European Union, which sets out this balance.

7 The European Convention on Human Rights is connected to the Council of Europe, a separate organisation with a wider membership than the EU.

8 The Charter states that:
"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. C*ompliance with these rules shall be subject to control by an independent authority.*"

9 The preamble also cites other fundamental rights such as "*respect for private and family life, home and communication… freedom of expression and information, freedom to conduct a business…*"

10 Preamble recital (13).



Article 1(3) of the GDPR underscores the weight given to the principle of free movement of personal data as it "*shall… neither be restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data*."

This reasoning stems from the principles of free movement within the EU. As repeatedly stated by the EU Courts, "*the free movement of goods, persons, services and capital are fundamental* [EU] *provisions and any restriction, even minor, of that freedom is prohibited*."[11] [emphasis added]

In sum, within the EU, both **the Charter and the GDPR acknowledge that while the protection of personal data is of fundamental importance, it is not an absolute right. Instead, the GDPR clearly strikes a balance between these rights and establishes that the free movement of personal data within the EU shall not be restricted more than what is set out in the GDPR**.

Personal data flows outside the EU allowed by the GDPR

The GDPR will have extraterritorial application. Article 3(2) makes clear that the GDPR shall apply to controllers and processors that are located outside of the EU if the processing of personal data relates to offering goods or services to, or monitoring the behaviour of, data subjects in the EU.

Perhaps more importantly, the GDPR imposes a general prohibition on transfers of personal data to countries outside of the EU, unless one of the three types of unilateral exemption regimes can be applied. These regimes give permission to transfers of personal data to third countries or to entities within a third country.

The first exemption, under Article 45 of the GDPR, permits transfers to countries that the EU Commission has decided have an "adequate level of protection" of personal data. In the newly-adopted Privacy Shield Decision (which replaced the former Safe Harbor Agreement), the EU Commission has decided to permit the flow of personal data to a number of self-certified private entities within the US. The second exemption regime allows for transfers falling under one of the so-called *safeguard* situations outlined in Article 46 where a transfer of personal data is allowed without the need for prior authorisation from the Commission (e.g. the use of binding corporate rules or model clauses adopted by the Commission). The third exemption is for transfers covered by a range of specific derogations outlined in Article 49.[12]

Article 44 introduces these provisions and explains that they are justified "*in order to ensure that the level of protection of natural persons guaranteed by* [the GDPR] *is not undermined*."

Thus, the GDPR is legally constructed to have extraterritorial application so as to ensure the same level of protection of personal data for those whose personal data is transferred to countries outside the EU. This is legally accomplished by (i) allowing the transfers (cross-border data flows) to certain third countries while at the same time (ii) setting procedures to verify and ensure the same level of protection in the third country as required in the EU under the GDPR.

Incentive for extraterritorial application of the GDPR

Allowing personal data to be transferred outside of the EU in the first place opens up the opportunity for the EU to impose its data protection standards in third countries, by incentivising countries or companies to adopt an equivalent standard of protection to ensure they are allowed to freely transfer data from the EU. Thus, arguably, one essential way in achieving this extraterritorial EU-level protection of personal data, is for the EU to permit, conditionally, cross-border transfers of data in the first place. Conversely, by disproportionally blocking transfers of personal data, the EU provides a disincentive for other countries to apply the EU's standard.

11 Case C-49/89, Judgment of the Court of 13 December 1989, *Corsica Ferries France v Direction générale des douanes françaises*, ECR [1989] p. 04441.

12 This exemption covers, for example, situations where the data subject has consented to the proposed transfer, the transfer is necessary for the performance of a contract or where the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject.

Arguably, therefore, there is an ultimate incentive to allow data flows, which may contain personal data. This would allow the EU to extend its data protection standard globally and would justify bringing the EU's data protection provisions into a bilateral or multilateral agreement. The EU's standard, instead of being applied *unilaterally* by the EU, could become a standard applied *bilaterally* or even *multilaterally* by many more countries.

In a bilateral or multilateral context, the EU should apply the legislator's reasoning of the GDPR i.e. the proportional balance between the fundamental right to protection of personal data and the free movement of such data within the internal market. Arguably, **the same balance should also be transposed into a bilateral or multinational agreement, meaning that when negotiating data protection requirements in an agreement, they should be coupled with provisions allowing the free movement of data (including personal data) between the countries**.

If the EU refrains from entering into any bilateral or multilateral negotiations and instead **continues to apply the GDPR unilaterally, there may be a higher risk that a WTO-member could resort to challenging the GDPR under WTO rules**. In the below section we therefore analyse the risk that the GDPR faces under a WTO scrutiny.

GDPR – consistency with WTO GATS XIV

Restrictions on data flows and the link to GATS

In the past, cross-border data transfers were normally related to the movement of a data medium (e.g. a CD or a hard drive). Data that was transferred separately would often be linked to the export of a physical product (e.g. maintenance data from exported products). **Due to the rapid technical development in recent years, the majority of cross-border data transfers are completely independent from any movement of physical goods. Nowadays it is more likely that such transfers would be linked to cross-border services. Therefore, in the absence of a WTO agreement on data flows, a WTO challenge to the GDPR would likely be made with reference to GATS**.

GATS does not mandate the free movement of services in general terms but instead binds a WTO member to permit free access to services in the specific sectors indicated in each member's "schedule of specific commitments". The EU's schedule does not expressly cover data flows as a service, but lists different types of services, for which free data flows may either support or are a necessity for the service (e.g. the section Computer and Related Services).[13] A challenge would therefore have to be brought against a specific service commitment in the EU's schedule. The complaining WTO member would have to show that the service is impeded by the EU's restrictions on data flows (e.g. accounting services and data related to personal income).[14] Arguably therefore, a number of GATS-covered service sectors, that rely on data flows could potentially be used as gateways for a WTO challenge.

A complaining WTO member would have to show that the GDPR breaches the commitments in GATS. The GDPR's system of unilaterally deciding on permitted transfers to specific countries ("**Adequacy Decisions**"), risks **being deemed a breach of the principle of Most Favoured Nation** ("**MFN**") under GATS Art. II:1 as other WTO member countries are not automatically awarded the same rights to data transfers as the countries covered by the Commission's Adequacy Decisions. Further, the way in which the GDPR is applied **also risks breaching GATS Art. VI which mandates that domestic regulations are applied in a reasonable, impartial and objective manner so as not to impede trade in services**. The burden of proof would then lie on the EU to justify the use of that system, under one of the GATS exceptions; general under GATS Art. XIV, national security or GATS Art. V for regional integration. In the section below we will focus on GATS Art. XIV.

GATS Art. XIV allows a WTO member to apply measures contrary to MFN when they are, *inter alia*, "necessary" to maintain public order (Article XIV (a)) or "necessary" to secure compliance with laws or regulations that are not WTO-inconsistent and that relate to the protection of the privacy of individuals in relation to processing and dissemination of personal data (Article XIV (b)(ii)). **Regardless, even if justified under these provisions, the measures may not be applied in a manner that is "arbitrary or unjustified" between countries where "like conditions prevail" which is a precondition for justifying any exception** under Article XIV (the Art. XIV "**Chapeau**").

Necessity test for the protection of privacy and personal data

Importantly, an evaluation of whether the GDPR's restrictions to data flows are justified under GATS Article XIV (b)(ii) would include a **test of necessity**. Here, a panel or Appellate Body would weigh various factors to determine whether the measure is necessary in order to achieve the stated objective. This would include an assessment of the importance of the objective, the contribution of the measure to the objective, and the trade-restrictiveness of the measure trying to achieve the objective. **The greater the measure's restrictive effect on trade, the greater the need to demonstrate that the measure serves the objective**. The review would also involve an assessment of **whether less trade-restrictive measures might have been possible**.[15]

13 The EU's schedule of specific commitments contains several sub-sections to the section on Computer and Related Services and includes, for instance, Data Processing Services (CPC 843) and Software Implementation Services (CPC 842). However, the EU has restricted the scope of these services, and excludes from this section, other services related to computers. In a footnote to this section the EU explains that "[I]*n many cases, computer and related services enable the provision of other services* by both electronic and other means. However, in such cases, there is an important distinction between the computer and related service (e.g., web-hosting or application hosting) and the other service* enabled by the computer and related service. The other service, regardless of whether it is enabled by a computer and related service, is not covered by CPC 84*." [* gives examples of accounting, auditing and bookkeeping services, architectural services, medical and dental services]. http://trade.ec.europa.eu/doclib/docs/2012/november/tradoc_150087.pdf

14 The WTO member would also have to show that the service occurs under one of the four modes of supply as proscribed in GATS.

15 See WTO Appellate Body Report, *US – Gambling*, WT/DS285/AB/R, paras.

In a review of the GDPR, therefore, the EU would have to show that the restrictions on data flows (the trade-restrictive measure) are necessary to achieve the protection of personal data of EU persons in third countries (the objective). When looking at the importance of the objective (protecting personal data), it is likely that a **panel or Appellate Body would look at the EU legislator's assessment and reasoning as stated in the preamble to the GDPR, where, as is set out above, the protection of personal data is not absolute and must "be balanced against other fundamental rights, in accordance with the principle of proportionality"**.[16] It is therefore conceivable that a panel or Appellate Body would require a higher level of justification to show that (i) the trade restrictions in the GDPR are necessary, and (ii) that there are no less restrictive measures available to achieve the protection of personal data.

The Chapeau: arbitrary or unjustifiable discrimination where like conditions prevail

Separately from passing the necessity text, **the EU would have the burden of proof to show that the GDPR's regimes, which result in data transfers being allowed to certain countries and entities only, do not result in an arbitrary or unjustifiable discrimination between countries where like conditions prevail**. Such a review would focus both on how the legislation is drafted and how the regimes are actually applied. As explained by the WTO Appellate Body, these Chapeau-rules "*serve to ensure that*... [Members use the] *exceptions reasonably, so as not to frustrate the rights accorded to other Members*."[17]

As the Adequacy Decisions evidently discriminate (by providing favourable decision toward some countries only), **the EU would have to prove a justification for that treatment, i.e. between positive and negative Adequacy Decisions**. One difficultly might be the EU's willingness to negotiate the new Privacy Shield, allowing the EU to take a favourable Adequacy Decision towards the US, which could be viewed as arbitrary or unjustified because the EU does not negotiate such agreements with every country before taking an Adequacy Decision.[18] **Another potential difficulty lies in the discrimination between countries with favourable Adequacy Decisions, and countries for which no decision has (yet) been taken, but where "like conditions" (i.e. a similar level of data protection) actually may prove to exist**. This in turn may also raise the question of whether the EU adequacy review is too strict (e.g. requiring that the standard of data protection is equivalent) as the term "like conditions" could be interpreted broader and include other similar but slightly differentiated standards. Thus, even if WTO case law on the GATS Art. XIV Chapeau is scare, the unilateral nature of the EU's Adequacy Decisions and how the **EU applies the regime in practice, arguably makes the GDPR vulnerable to scrutiny under the test of arbitrary or unjustifiable discrimination**.

In conclusion, the EU faces a risk that the GDPR is challenged in the WTO as being inconsistent with GATS article XIV, by being too trade restrictive in proportion to the intended purpose of protecting personal data.

GDPR, TTIP, and the Trans-Pacific Partnership ("TPP")

Although, at present, the EU has not proposed any narrative concerning the protection of personal data in the TTIP negotiations, the US's likely position is reflected in the relevant provisions of the TPP. These provisions are considered below.

The principle of free data flows in general in TPP

Chapter 14 of TPP, entitled Electronic Commerce, is designed to ensure the free flow of data, to prevent localisation requirements, to protect consumers, and to ensure privacy. In other words, it sets down plurilateral trade law rules pertaining to the free movement of data flows.

Article 14.11 of the TPP deals with cross-border transfers of information by electronic means. The article recognises that each party has the right to its own regulatory requirements for such transfers, while also establishing a principle of free movement as each party "*shall allow the cross-border transfer... including personal information.*"

304 to 311. Importantly, the Appellate Body ruled that there is no obligation, under the necessity test, to consult or agree with another member to find a less trade restrictive measure, see para. 317.

16 Based on the Appellate Body's ruling in *US – Gambling*, how the EU characterizes the GDPR's objectives and its effectiveness, "*will be relevant in determining whether the measures is, objectively, "necessary.*" Even so, a panel is not bound to these "*characterizations... and may also find guidance in the structure and operation of the measure and in contrary evidence proffered by the complaining party.*" *Ibid.* para. 304.

17 *Ibid.*, para. 339.

18 Although based on *US – Gambling*, para. 317, there is no requirement to negotiate a less trade restrictive measures, the practice of doing so with some countries only would appear discriminatory.

Article 14.13 deals with computer localisation requirements. The article first recognises that each party has the right to its own regulatory requirements as regards the use of computing facilities, while also establishing a principle of freedom of establishment of equipment, stating that no party shall require anybody to "*use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.*"

Under both 14.11 and 14.13, each party has a right to adopt measures which could block or hamper such transfers or impose localisation requirements, in order to achieve a "*legitimate public policy objective*", provided the laws do not constitute "*(a) arbitrary or unjustifiable discrimination or a disguised restriction on trade*", and that such measures are (b) proportionate ("*not... greater than... required to achieve the objectives*").

TPP and GDPR consistency

The TPP provisions are constructed similarly to that of the GATS XIV language, and it is conceivable that a dispute resolution panel would seek interpretation from WTO reports on GATS XIV and GATT XX. **The key question therefore, is whether the EU would face an additional risk in concluding a TTIP agreement with similar language to the TPP, given that the US could readily challenge the GDPR provisions restricting data flows in the TTIP's associated dispute resolution mechanism**.

On the one hand, there would be a clearer link between the TPP provisions and the GDPR, as there are clear obligations in the TPP relating to the free movement of data. This is in contrast to the difficultly of assessing data flows as a service under GATS. **Thus, any challenge to the GDPR would be more likely to be deemed admissible in a bilateral dispute resolution mechanism than before the WTO panel**.

As regards the substantive assessment, i.e. whether a claimed restriction would be justified under Articles 14.11 or 14.13, a bilateral dispute resolution mechanism would likely review whether the GDPR restrictions on transfers of data would be proportionate in relation to the objective (i.e. protection of personal data). Again, it is then conceivable that the panel examines the rationale of the EU legislator when adopting the GDPR and the balance struck between the principles of freedom and protection enshrined in Articles 1(2) and 1(3) of the GDPR.

Conclusions on safeguarding GDPR through TTIP

Mitigating inherent risks by entering into bilateral or multilateral negotiations

The GDPR already faces an inherent risk of being successfully challenged under current WTO rules. The US, or any other WTO member, could challenge the GDPR as a domestic regulation inconsistent with GATS. A review of whether the **GDPR's restriction on trade is justified** under the exceptions in GATS XIV, would likely include a weighing of the restrictiveness of the measure (restriction on transfers of data) against the achieved objective (protection of personal data) and a proportionality test would also be performed. Further, the EU would have to prove that the application of the GDPR **does not lead to an arbitrary or unjustified discrimination between countries** where similar standards apply, so as to ensure that the exception is used in a reasonable way.

A legal review of necessity and proportionality, as well as of reasonability, are by nature an exercise in balancing different factors, and the outcome will, in many cases, depend on what the claiming or responding party is able to demonstrate. Thus, a WTO complaining party would show the restrictiveness of the GDPR, and the EU would have to demonstrate the contrary, that the service is not restricted, or at least that any restrictions arising from the GDPR are proportionate, necessary and reasonable.

One way of balancing such tests of necessity, proportionality or reasonability, in favour of supporting the existing GDPR restrictions on personal data, would be to formulate transparent and favourable rules for data flows in general between the EU and other countries. That would arguably change the general perception of the GDPR, i.e. that the EU's restrictions on data flows containing personal data is a specific and justified exception from a broader and more general principle allowing free data flows (that do not contain personal data). **It may also lead to a lessening or a shift in the burden of proof, under a possible WTO or other dispute mechanism review**, as the complaining party would have to show *de facto* that data flows are actually being hampered.

Arguably, therefore, **it is in the long-term interest of protecting the GDPR to formulate a position in favour of the free flow of data to and from the EU, with the aim of introducing it in a bilateral or multilateral context**.

This report focuses on the option of formulating a position in the TTIP context (bilateral negotiation). The EU could, and arguably should, in parallel, presents its position in the on-going plurilateral negotiations of the new Trade in Services Agreement ("**TiSA**"). This report does not further analyse the EU's possible political reasons or negotiating strategies of promoting one or the other. Based on the above reasoning however, it would be beneficial for the GDPR if the EU were to start shifting in the near future from applying a unilateral standard, to a bilateral or multilateral standard.

Negative consequences of not formulating a position

By not formulating a position or entering into any bilateral or multilateral negotiations on such a text, **the EU will continue to act unilaterally under the GDPR**. As noted above, as more service sectors become dependent on free data flows, **the more potential GATS challenges could be triggered under the EU's services schedule**. Also, as the number of countries subject to Adequacy Decisions increases, so too does the **potential for diverging and arbitrary discrimination, leading to a larger pool of possible WTO members complainants**. Therefore, arguably, the longer the EU continues to act unilaterally, the higher the risk of potential challenges to how the GDPR is applied.

Positive effect of formulating a position, preferably in the TTIP

Presenting a negotiating position in the TTIP permitting the free movement of data **does not automatically mean renegotiating or lowering the data protection standards set out in the Privacy Shield**. Rather, the EU could in fact strengthen the GDPR in the transatlantic context, as the EU could propose text to delineate clearly between the right to free movement of data and the obligation to protect personal data in the TTIP. In other words, the EU does not need to accept the language of the TPP and the existing Privacy Shield need to not be renegotiated for this reason. Furthermore, even looking at the TPP language, the US position is to permit domestic regulations for protecting personal data.

The advantage of presenting a negotiating position in any bilateral context is that it can be replicated in other bilateral free trade negotiations. This is common EU practice in negotiating free trade agreements. Furthermore, the **dignity of the TTIP agreement, i.e. between two major trading blocks, could set an international standard**, which could be replicated in other bilateral or multilateral free trade agreements, to which the EU or US is a party, but also between two or more other third countries.

In turn, a bilateral agreement such as the TTIP, could foster the WTO "building block principle" and could encourage a specific multilateral or plurilateral agreement on data flows, under the auspices of the WTO. A specific section in the TTIP could also set the standard for a specific section on data flows in the ongoing negotiations of TiSA. This could eventually be extended to all WTO members if a sufficient number of members adhere to such an agreement.

Therefore, **arguably, presenting a negotiating text in TTIP, which allows free data flows, while delineating and protecting transfers of personal data, is both timely and of strategic value for the long-term application of the GDPR and the extension of EU data protection standards internationally**.

This report has been commissioned by LM Ericsson.

STOCKHOLM
NORRLANDSGATAN 21
BOX 1711
111 87 STOCKHOLM

GÖTEBORG
ÖSTRA HAMNGATAN 16
BOX 2235
403 14 GÖTEBORG

MALMÖ
CARLSGATAN 3
BOX 4291
203 14 MALMÖ

HELSINGBORG
SÖDRA STORGATAN 7
BOX 1384
251 13 HELSINGBORG

MOSKVA
ROMANOV DVOR BUSINESS CENTRE
ROMANOV PER. 4
125009 MOSKVA, RYSSLAND

SHANGHAI
25/F, PLATINUM
NO. 233 TAICANG ROAD, LUWAN DISTRICT
SHANGHAI 200020, KINA

HONG KONG
33/F, JARDINE HOUSE
1 CONNAUGHT PLACE
CENTRAL, HONG KONG, KINA

BRYSSEL
IT TOWER
AVENUE LOUISE 480
1050 BRYSSEL, BELGIEN

NEW YORK
101 PARK AVENUE
NEW YORK NY 10178, USA

MANNHEIMERSWARTLING.SE

Mannheimer Swartling is the leading commercial law firm in the Nordic region with an international practice and assignments all over the world. By combining the highest legal competence with industry know-how, we offer our clients professional legal advice with added value.

MANNHEIMER SWARTLING