



**Stanford – Vienna
Transatlantic Technology Law Forum**

A joint initiative of
Stanford Law School and the University of Vienna School of Law



TTLF Working Papers

No. 39

**Cross Border Data Transfers Under the
GDPR: The Example of Transferring Data
from the EU to the US**

Nikolaos I. Theodorakis

2018

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology-related and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at <http://ttlfs.stanford.edu>. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
<http://ttlfs.stanford.edu>

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Nikolaos Theodorakis is a Lecturer and Fellow at the University of Oxford and a senior associate with Alston & Bird LLP, focusing on issues of privacy and data protection, technology, international trade law and competition law. Nikolaos completed his Ph.D. at the University of Cambridge, where he focused on issues of Corporate Compliance, Liability and Regulation. He also holds degrees from the University of Athens (LL.B.), University of Cambridge (M.Phil.), University of Oxford (PGC), London School of Economics (B.Sc.) and University College London (LL.M.).

Prior to joining Oxford, Nikolaos taught and conducted research at the University of Cambridge, Harvard Law School, and Columbia Law School. Nikolaos has further worked for the U.S. Committee on Capital Markets Regulation, the Legislative Committee at the U.S. Congress and the Library of Congress, and the UK Sentencing Council. Nikolaos has received fellowships and awards from the ESRC, the British Academy, the Greek Parliament, the Greek State Scholarships Foundation, the EU Bursaries and the Corfield foundation, among others. He has published papers on various topics and presented extensively in conferences and symposia.

Nikolaos's recent engagements include serving as a UN international consultant and legal trainer, an OECD expert, an EU Commission international expert, and a Transparency International country assessor. In the past, he has also assumed research and teaching fellowships with Harvard University, the Institute of Advanced Legal Studies at the University of London, the British Institute of International and Comparative Law, and the Max Planck Institute of Foreign and International Criminal Law.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:

Nikolaos I. Theodorakis, Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US, Stanford-Vienna TTLF Working Paper No. 39, <http://ttlfs.stanford.edu>.

Copyright

© 2018 Nikolaos I. Theodorakis

Abstract

The General Data Protection Regulation recognizes specific options for data transfers between the EU and the US. Since the European Commission does not fully consider the US a data “adequate” country because of its lack of comprehensive privacy legislation, different instruments need to be in place for a legitimate data transfer. Such instruments include Binding Corporate Rules, European Commission model clauses, certification mechanisms, codes of conduct, and other recognized adequacy mechanisms. One of them is the EU-US Privacy Shield Framework.

The EU-US Privacy Shield Framework was designed by the U.S. Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce. The European Commission deemed the Framework adequate to enable data transfers under EU law in July 2016. To join the program, a US based organization needs to self-certify and publicly commit to comply with the Framework’s requirements.

This paper investigates the various cross-border data transfer mechanisms provided in the GDPR and discusses how organizations in the US can use them to transfer data from the EU.

Contents

I. Adequacy Determinations of the European Commission.....	6
1. Transfers to Jurisdictions Offering “Adequate Level of Protection”	7
2. Will the UK be recognized as an equivalent country after Brexit?	11
3. Is Adequacy in line with the WTO?	13
4. What about the US? Safe Harbor and Privacy Shield.....	18
a. Background: Safe Harbor.....	18
b. Privacy Shield	18
c. Privacy Shield Principles	19
d. Privacy Shield Enforcement	23
e. First Annual Review of the EU-US Privacy Shield.....	24
II. Transfers on the Basis of “Appropriate Safeguards”	26
1. Model Clauses.....	27
a. Next Steps and Practical Expectations.....	30
2. Binding Corporate Rules (“BCRs”).....	32
a. BCRs under the Directive	32
b. BCRs under the GDPR	33
3. Codes of Conduct and Certifications	36
a. Codes of Conduct.....	37
b. Certifications.....	39
III. Derogations	42
1. Consent	44
2. Other Derogations	45
3. A New Ground: “Compelling Legitimate Interests” of the Controller.....	46
IV. Penalties for Non-Compliance.....	48
V. Conclusion	49

The EU's General Data Protection Regulation ("GDPR") entered into force in May 2018. It is the most significant legal development in the sphere of privacy and data protection in the EU over the past 20 years. It standardizes certain procedures, sets a paradigm for what is expected from companies and individuals processing personal data, and enhances the individuals' rights in an effort to ensure they maintain control over how their data are collected and used.

One of the questions at the top of most companies' agenda is what effect the GDPR will have on transatlantic data flows. Every second that goes by companies transfer data from the EU to the US to manage their IT systems, sell and buy products and services, manage their personnel, engage in marketing activities, use the cloud for their operations, create new value chains, comply with law and report to the authorities, and many more purposes. The global economy is largely based on cross-border data transfers since data is the oil of the 21st century and the driving force behind profit and growth for every corporation.

The global economy is largely interconnected. This is related to the so-called fourth industrial revolution that refers to end-to-end digitization of all assets and integration into a digital ecosystem.¹ Cross-border data access is essential to ensure economic growth. Every sector relies on the global flow of data and takes advantage of the economies of scale that produce efficiencies due to this data flow. The expectation is, further that the increase of cross-border data transfers further allows users to make use of new technologies, increase market efficiency, reduce market barriers to market entry, and allow small and medium sized enterprises to enter disproportionately large markets.

¹ See Schwab 2016 Market Outlook Report

Global data flows are overall transforming the nature of international trade from selling goods and services to participating in global value chains. McKinsey & Company estimates that global data flows raised global GDP by about 3.5 percent over what would have occurred without such flows, equivalent to \$2.8 trillion dollars in 2014, a figure that could reach \$11 trillion by 2025.² In the United States in particular, digital trade has raised GDP by 3.4-4.8 percent by increasing productivity and lowering the costs of trade; it has also increased wages and contributed to creating as many as 2.4 million new jobs.³

Further, a recent World Bank study found that a 10 percent increase in internet penetration in the exporting country leads to a 1.9 percent increase in exports along the quantity of goods, and a 10 percent increase in internet penetration in the importing country leads to a 0.6 percent increase exports along the intensive margin (the average value of goods).⁴

If digital trade facilitated through cross-border data flows is so beneficial, then why do governments increasingly restrict it? Well, for a number of reasons that range from ensuring that other countries furnish adequate protections to the data, to ensure rapid access by local law enforcement agencies, national security reasons, and to create a level playing field for local players. Data localization measures, as they are called, have economic and trade costs. Bauer et al found that the cost of proposed and enacted data localization measures in India, Indonesia and Vietnam would reduce GDP in India (-0.1 percent), Indonesia (-0.5 percent) and Vietnam (-1.7 percent).

² McKinsey & Company, Digital Globalization: The New Era of Global Flows, p. 13-18.

³ Castro, D. and McQuinn, A., Cross-Border Data Flows Enable Growth in All Industries, 2015, 11.

⁴ Osnago, A. and Tan, S. (2016), Disaggregating the impact of the internet on international trade, p. 4.

Data localization measures can take different forms, for instance that data cannot be transferred outside national borders (total prohibition) or that data can be transferred outside national borders, but a copy of said data must be kept locally (partial prohibition). Apart from data localization, which is quite radical, several countries opt instead for data restriction measures, meaning measures that restrict the cross-border flow of data. In such cases, the data exporter can only transfer such data across borders if the data importer meets specific criteria (e.g. they have signed an agreement known as model clauses in the EU, or they reside in an adequate country).

While every government can opt for the acceptable level of risk, data localization is suboptimal since it restricts digital trade and it introduces restrictions to growth. This leads, in sequence, to reduced exports.

Despite the benefits associated with free cross-border data flows, the default position in EU law has been to prohibit transfers of data to countries outside the EU, i.e. outside the digital single market. Even under the previous legal regime (the EU Data Protection Directive of 1995) data transfers to non-EU countries were only permitted when personal data received an “adequate level of protection” in the destination country.

The GDPR adopts the same approach since data transfers to non-EU countries are in principle prohibited. The GDPR recognizes certain mechanisms that can provide an exception and therefore legitimize the data transfers, including

- (i) an “adequacy decision” by the European Commission;
- (ii) EU-sanctioned “appropriate safeguards” for transfers such as model clauses; and

- (iii) statutory exceptions to the general transfer prohibition, such as consent or contractual obligations.

Additionally, the GDPR contains new transfer mechanisms such as (iv) certifications and (v) approved codes of conduct. The GDPR also formalizes Binding Corporate Rules (“BCRs”) as a legal basis for international data transfers, which already existed before but were not codified under the Data Protection Directive. To streamline the processes and reduce red tape, the GDPR ends prior-notification and authorization requirements that constituted significant administrative hassle for companies.

The GDPR establishes a clear hierarchy among its transfer mechanisms, signaling the ones that it prefers the most. Its ideal transfer mechanism is an adequacy decision issued by the European Commission (“Commission”). For this to happen, the Commission needs to formally declare that the destination country for a data transfer offers adequate data protection.⁵ The Commission favors countries that have codified their privacy rules in a single law and that ideally follow a similar approach as the EU does.

If no adequacy decision is available, the GDPR’s ‘second choice’ for transfer mechanisms are enumerated “safeguards” for data transferred abroad that have been approved by the Commission or by national data protection authorities. These include:

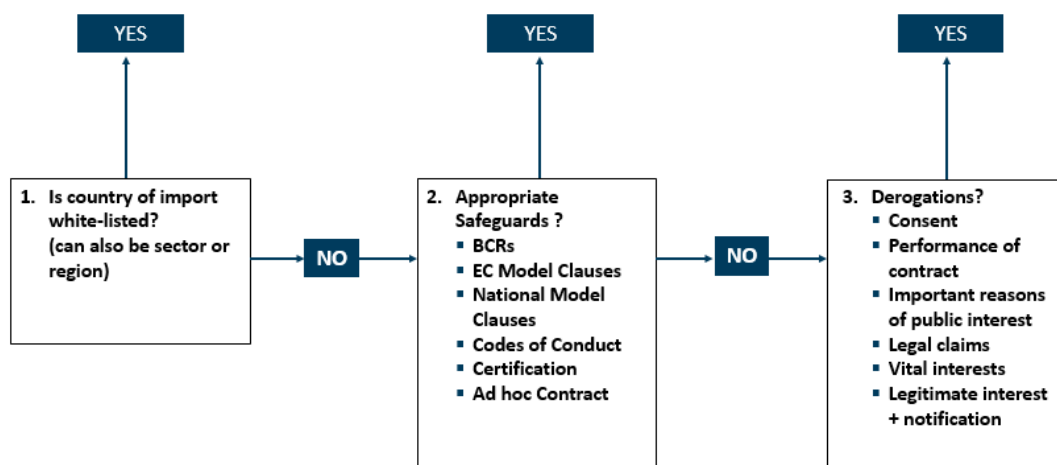
- model contractual clauses;
- binding corporate rules;
- accredited third-party certifications (such as privacy marks or seals);
- approved industry codes of conduct;

⁵ See Article 45(1) GDPR.

- and *ad hoc* data transfer contracts.

If no such “safeguards” are available, the GDPR’s clear ‘last choice’ for transfer mechanisms are an enumerated list of derogations permitting limited data transfers to non-EU countries.

Graphically represented, the GDPR’s transfer-mechanism hierarchy appears as follows:



In this paper, we will assess the international transfer mechanisms available under the GDPR and how the European Data Protection Board (“EDPB”, formerly known as Article 29 Working Party and used in this paper also as WP29 interchangeably) has further refined and interpreted how these derogations should apply in practice.⁶ We will also discuss the options that organizations have when they want to transfer data from the EU to the US and what are the things to consider before choosing the appropriate mechanism.⁷

I. Adequacy Determinations of the European Commission

⁶ Position of the Council at first reading with a view to the adoption of the Regulation of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal information and on the free movement of such data, April 6, 2016.

⁷ See Article 45 of the GDPR.

1. Transfers to Jurisdictions Offering “Adequate Level of Protection”

The European Commission (“Commission”) has statutory authority to determine that a non-EU jurisdiction offers an “adequate level of protection” for personal data.⁸ The Commission makes this determination through a so-called “adequacy decision” adopted after notice to and comment from representatives of EU Data Protection Authorities (“DPAs” or “SAs” to reflect the updated GDPR term of Supervisory Authorities). An adequacy decision is binding for all EU member states and permits unlimited data transfers to the country the Commission has designated as “adequate.” Over time, the Commission’s adequacy decisions have generated a “white list” of countries to which companies can transfer personal data without limitation.

In essence the standard to recognize equivalence is that the data will be handled with practically the same care in the third country as if they were in the EU (i.e. an intra-EU transmission of data). So far, the Commission has recognized the following countries as equivalent: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (only limited to the Privacy Shield Framework) as providing adequate protection. Adequacy talks are ongoing in Japan and South Korea. These decisions do not cover data exchanges in the law enforcement sector which are governed by the “Police Directive”.⁹

The adoption of an adequacy decision requires:

- A proposal by the European Commission;

⁸ See Article 25(6) of the Directive and article 45 of the GDPR.

⁹ See Article 36 of Directive (EU) 2016/680.

- An opinion of the European Data Protection Board;
- An approval from representatives of EU countries;
- The adoption of the decision by the European Commissioners

The GDPR continues the tradition granting the Commission authority to issue adequacy decisions permitting data transfers to non-EU countries. In fact, the GDPR expands and regulates the Commission's adequacy decision authority. In particular:

- In addition to letting the Commission declare that a non-EU country offers adequate data protection, the GDPR now permits the Commission to determine that a specific *territory* or *sector* within a third country offers an adequate level of protection.¹⁰ This means that sectorial data privacy legislation such as children's privacy laws or telecom privacy laws in a certain country may be declared adequate. This is an interesting carve out since we may experience in the future the Commission declaring that a sector in a country is adequate, without necessarily considering the entire country adequate. It does not, however, come without interpretation difficulties since it will likely create a new round of discussions as to what are the limits of each sector (e.g. where does the healthcare sector exactly end). The industries and the players within the sectors are so interconnected that this may not be an easy qualification to make.
- The GDPR sets forth new minimum factors the Commission must consider when issuing an adequacy decision,¹¹ in particular:

¹⁰See Article 25(6) of the Directive.

¹¹ See Article 45(2) of the GDPR.

- The destination country's statutes and case law on data protection, national security, and onward transfers and how they have been implemented and enforced in practice;
- Effective and enforceable data subject rights in the destination country;
- The existence (or lack thereof) of independent supervisory authorities in the destination country that are responsible to ensure and enforce compliance with data protection laws;
- Any international commitments regarding data protection the destination country has entered into.

Historically, it appears that the Commission particularly weighs in the onwards transfer regime, the data subject rights and the potential access by state authorities of the data transferred when assessing whether a third country is adequate. The GDPR provides that the Commission's decisions are dynamic and must be reviewed at least every four years.¹² The Commission is also expected to monitor whitelisted countries "on an ongoing basis" to see if circumstances arise that would affect its adequacy decision.¹³ Given the dynamic nature of the adequacy decision, and the importance of said adequacy, the Commission retains full power to revoke an adequacy decision at any time after giving the affected jurisdiction notice and an opportunity to respond.¹⁴

Importantly for businesses, the GDPR provides that adequacy decisions the Commission made under the Directive will continue to apply until they are amended, replaced or repealed.¹⁵ This means that the Commission's "white list" of permissible destination countries will remain valid

¹² See Article 45(3) of the GDPR.

¹³ See Article 45(5) GDPR.

¹⁴ *idem*

¹⁵ See Article 45(9) of the GDPR.

under the GDPR, at least for the near term. Moreover, any adequacy decision the Commission adopts in the next two years—such as the Privacy Shield framework discussed below—will also remain in force in the GDPR era. Equally, the WP29 recently published an opinion that sets out the adequacy procedures after May 2018, which does not substantially alter the practice compared to the previous legal regime.¹⁶

Still, some legal uncertainty remains. Decisions of the European Court of Justice have established that a Commission adequacy decision is only valid if the data protection law in the destination country is “essentially equivalent” to EU law. Moreover, as stated above, the Commission is required to monitor the validity of its adequacy decisions “on an ongoing basis.”¹⁷

It is unlikely the Commission will begin publicly questioning its own adequacy decisions, however it issued a Communication in the beginning of 2017 that discusses its position regarding adequacy decisions and how they should be reached. Along with the Communication the Commission endorsed horizontal provisions for cross-border data flows and personal data protection in trade negotiations. This was a result of the Commission experiencing data protection often being subject to negotiations in the context of EU trade agreements. As the EU perceives personal data protection as a fundamental right, data flows between the EU and third countries can be ensured using the mechanisms provided under the EU data protection legislation. The Commission believes that dialogues on data protection and trade negotiations can complement each other but must follow separate tracks, like with Japan and South Korea.

¹⁶ WP254 on Adequacy Referential, Adopted on 28 November 2017

¹⁷ See Article 45(4) GDPR.

The Commission has tried to disassociate data protection and adequacy decisions as a leverage used in trade negotiations. In fact there have been allegations in the past whereby, anecdotally, countries have suggested conceding in certain trade negotiations in exchange to an adequacy decision by the Commission. The Commission wants to remove data protection as a bargaining chip and deal with this issues on a separate track, through separate adequacy negotiations. Apart from the EU's position that data protection is a fundamental right, it can also leverage higher data protection standards as a competitive advantage.

However, this position is not ideal. The Communication by the Commission includes a series of normative criteria before opening adequacy negotiations with third parties which include trade/political relations with a third country, the role of the third country in promoting data privacy and the overall political relationship with the country in question.¹⁸ These highly normative criteria relate more to a political than a legal decision as to whether a third country has an adequate level of data protection.

Based on these normative criteria, the Commission plans to engage in adequacy discussions with trading partners in East and South-East Asia, and, depending on the modernization of its data protection laws, with India and Mercosur countries. This highly political agenda resembles a trade negotiation agenda rather than a fundamental human rights based approach.

2. Will the UK be recognized as an equivalent country after Brexit?

¹⁸ COM(2017) 7 final, Communication Exchanging and Protecting Personal Data in a Globalised World , p.8

In short, no one knows. The Information Commissioner's Office (the UK's DPA) published an International Strategy 2017-2021 document¹⁹ where it lays out the priorities and objectives connected to data protection during the GDPR enforcement and after the UK has exited the EU (Brexit). The ICO introduces the concept of the UK as a "global data protection gateway"- a country with a high standard of data protection law which is effectively interoperable with different legal systems that protect international flows of personal data.

The ICO has further stressed its eagerness to contribute to the EDPB while the UK remains in the EU, however the EU's chief Brexit negotiation has made it clear that the ICO cannot remain in the EDPB after Brexit.²⁰ While the UK recognizes the importance of data flows, and the ICO is committed to work to ensure that personal data transferred from the UK to third countries continue to be adequately protected, no one can say for sure whether the Commission will find the UK an adequate country for GDPR purposes. Albeit this is a legal qualification rather than a political one, at least in theory, it is likely that an adequacy decision will depend on the Brexit terms.

In August 2017, the UK Government issued a paper titled "The exchange and protection of personal data- a future partnership paper", in which the Government states the following:²¹

"After the UK leaves the EU, new arrangements to govern the continued free flow of personal data between the EU and the UK will be needed, as part of the new, deep and special partnership. The UK starts from an unprecedented point of alignment with the EU. In recognition of this, the UK wants to explore a UK-EU model for exchanging and protecting

¹⁹ Information Commissioner's Office, International Strategy 2017-2021, p.2, available at: <https://ico.org.uk/media/about-the-ico/documents/2014356/international-strategy-03.pdf>

²⁰ Speech on 26 May 2018 to the 28th Congress of the International Federation for European Law, Michel Barnier.

²¹ HM Government, The exchange and protection of personal data : a future partnership, p. 2, available at : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf

personal data, which could build on the existing adequacy model, by providing sufficient stability for businesses, public authorities and individuals, and enabling the UK's Information Commissioner's Office (ICO) and partner EU regulators to maintain effective regulatory cooperation and dialogue for the benefit of those living and working in the UK and the EU after the UK's withdrawal."

However, despite the support for seeking an adequacy decision and the UK's efforts to align with the GDPR in its Data Protection Act 2018, there are concerns that an adequacy decision could actually be difficult to obtain due to the existence of the Investigatory Powers Act (IPA), which provides UK law enforcement and intelligence agencies with surveillance powers and has been widely criticised and challenged.

In case the UK is not considered an adequate country after Brexit, the UK will need to figure out alternative data transfer mechanisms to allow such transfers to EU countries. This will likely affect several companies, however at the writing of this chapter the likelihood of adequacy or non-adequacy is still unclear.

3. Is Adequacy in line with the WTO?

In the past, cross-border data transfers referred primarily to the movement of a data medium (e.g. a hard drive). Nowadays the majority of cross-border data transfers are de-attached from a movement of physical goods and relate more to provision of services. The World Trade Organization (WTO) does not have a special agreement on data flows, so any GDPR related issue taken up with the WTO would need to relate to GATS (General Agreement on Trade in Services). GATS entered into force in 1995 and binds WTO members to permit free access to

services in specific sector. The EU has assumed schedule specific commitment that relate to services where cross-border data flows are required (e.g. Computer and Related Services).²² A natural question is, hence, whether a complaining WTO member could file a complaint against the EU on the basis that the service is impeded because of EU's restrictions on data flows.

This hypothetical argument could further stipulate that adequacy decisions is a unilateral decision that permits transfers to specific countries, therefore allowing the seamless provision of the services to these countries whereas it introduces protectionist measures (i.e. cross-border transfers are restricted) to the non-equivalent countries. This discrimination arguably is in breach of the Most Favored Nation ("MFN") principle²³ which provides that a country needs to extend to the other countries the most favored treatment that it furnishes a third country. In this case the MFN principle would require that the EU would extend the adequacy preferential treatment to all the other third countries, otherwise it creates an uneven level playing field.

Further, the GDPR would risk 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 Commission's likely reaction is that the adequacy decision is not a matter of trade but rather an issue of fundamental human rights. As such, it would likely try to invoke the exception under GATS Art. XIV on national security. Such exception allows a WTO member to apply measures contrary to MFN when they are:

- (a) necessary to protect public morals or to maintain public order;*
- (b) necessary to protect human, animal or plant life or health;*

²² Data Processing Services (CPC 843) and Software Implementation Services (CPC 842).

²³ GATS Art. II :1

(c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: (i) the prevention of deceptive and fraudulent practices or to deal with the effects of a default on services contracts; (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; (iii) safety;

(d) inconsistent with Article XVII, provided that the difference in treatment is aimed at ensuring the equitable or effective imposition or collection of direct taxes in respect of services or service suppliers of other Members;

(e) inconsistent with Article II, provided that the difference in treatment is the result of an agreement on the avoidance of double taxation or provisions on the avoidance of double taxation in any other international agreement or arrangement by which the Member is bound.

The EU would have the burden of proof to demonstrate that adequacy decisions are justified under one of these exceptions. Even if they were, the measures may not be applied in an “arbitrary or unjustified” way between countries where “like conditions prevail”.²⁴

The most likely exception that the EU would invoke to justify adequacy decisions would be Article XIV(c)(ii) regarding the protection of the privacy of individuals. This argument would then be subject to scrutiny under the necessity test. A panel and perhaps consequently an appellate body would factor in the variables that determine whether the measure is necessary to achieve its stated objective. Based on past case law of the WTO this test would include an assessment of the importance of the objective, the contribution of the measure to the objective,

²⁴ This is a general precondition for applying any exception under Article XIV.

the trade-restrictiveness of the measure trying to achieve the objective.²⁵ The review would also involve an assessment of whether less trade-restrictive measures might have been possible.²⁶

In a potential GDPR review under the WTO the EU would have to show that data flow restrictions are required to achieve the protection of personal data of EU persons in third countries. As part of the judicial review, the panel body would likely also review the GDPR preamble where personal data protection is not absolute. Rather, it needs to “be balanced against other fundamental rights, in accordance with the principle of proportionality”.²⁷ A panel body could therefore potentially find that the trade restrictions in the GDPR are necessary and (more importantly) that the adequacy decisions do not violate the MFN principle.

A core argument in such legal challenge would be that the adequacy decision can be considered a valid exception only if there are no other ways to achieve the protection of personal data. However the GDPR provides a number of other ways to transfer data abroad (e.g. consent), which potentially neutralizes the necessity argument. If it is necessary to restrict data transfers abroad to non-adequate countries, which creates the need to have unilateral adequate decisions, then why are there other exceptions to transfer data abroad? Conversely, does not the adequacy decision create an uneven playing field, therefore preferring some countries over others and violating the MFN principle?

In essence this is a question of classification. If the Commission argues that personal data protection is a fundamental right, then adequacy decisions are connected to said right and no

²⁵ WTO Appellate Body Report, US – Gambling, WT/DS285/AB/R, paras. 304 to 311.

²⁶ 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.

²⁷ WTO Appellate Body Report, US – Gambling, WT/DS285/AB/R, paras. 304 to 311.

further exceptions should be allowed (i.e. you strictly regulate this fundamental right to justify the necessity of unilateral actions). However, this does not reflect the present GDPR reality, which creates an inherent inequality between states. If the Commission argues that personal data can be seen as a commodity, to an extent, regarding the provision of cross-border services and justifies the adequacy decisions as a trade preferential tool, this also comes in direct violation of the MFN principle.

Further, and irrespective of passing the necessity test, 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 only, do not directly result in an arbitrary or unjustifiable discrimination between countries. As the adequacy decisions discriminate by providing favorable decision toward some countries only, the EU would have to prove a justification for that treatment, i.e. between positive and negative Adequacy Decisions.

Finally, the EU would need to explain the balancing legal test and the difference between the countries for which it has issued favorable adequacy decisions and countries for which no decision has yet been taken. These countries may have like conditions, meaning a similar level of data protection and this may in turn raise the question of whether the EU should have afforded the same adequacy to all like countries.

In practice, the WTO has not dealt with many cases connected to GATS Art. XIV so far. The unilateral nature of the EU's adequacy decisions however arguable makes the GDPR vulnerable to scrutiny under arbitrary or unjustifiable discrimination. If a country were to ever challenge the adequacy decision regime based on WTO rules, it would lead to an interesting legal debate.

4. What about the US? Safe Harbor and Privacy Shield

a. Background: Safe Harbor

Most U.S. organizations that receive EU data either used or were familiar with the Safe Harbor framework (“Safe Harbor”). Safe Harbor was a transfer mechanism negotiated between the Commission and the U.S. Department of Commerce (“DOC”) that, for years, was the basis for a Commission adequacy decision finding that the U.S. provided an “adequate level of protection.” Under Safe Harbor, companies that self-certified they would comply with certain data-protection principles were permitted to transfer personal data from the EU to the U.S.

Safe Harbor was a very popular transfer mechanism that 4000+ of American companies took advantage of it to legitimate their transatlantic data transfers. Some European DPAs have historically however always criticized Safe harbor for not offering true “adequacy” especially with respect to transfers to data processors and onward transfers. Following the Snowden revelations Safe Harbor fell under even more criticism as it did not provide sufficient protection against U.S. surveillance. In the *Schrems* landmark decision of October 6, 2015,²⁸ the EU Court of Justice (“ECJ”) invalidated Safe Harbor on the basis of surveillance concerns (albeit not formally). As a consequence, thousands of businesses rushed into alternatives to transfer personal data to the US, and fell generally back onto EU Model Clauses.

b. Privacy Shield

²⁸ *Maximilian Schrems v. Data Protection Commissioner*, case C-362/14, European Court of Justice.

The EU-U.S. Privacy Shield (“Privacy Shield”) replaced Safe Harbor in 2017. In February 2016, the Commission, the DOC, and the Federal Trade Commission (“FTC”) released a 130-page package of Privacy Shield documents. Like Safe Harbor, Privacy Shield is a self-certification regime that permits any company that self-certifies to abide by the Privacy Shield Principles to transfer personal data from the EU to the US. The Privacy Shield includes obligations for US companies receiving personal data from the EU, as well as obligations for the US government if they subsequently request access to this personal data for national security or law enforcement reasons, in response to the Schrems case that led to the initial invalidation of the Safe Harbor. The arrangement also gives EU individuals the right to make a complaint if they think that their personal data is not being properly protected.

c. Privacy Shield Principles

Companies that self-certify with the Privacy Shield commit to comply with the Privacy Shield Principles. The Privacy Shield Principles are similar to the principles that existed under Safe Harbor, in particular:²⁹ Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; Recourse, Enforcement, and Liability.

However, Privacy Shield expands the compliance obligations and liability that existed under Safe Harbor. The following are the more salient changes under Privacy Shield.

²⁹ The draft opinion must be reviewed by the EU Data Protection Supervisor and the EU Member States prior to finalization by the EU Commission.

- (i) Notice – Companies must provide “clear and conspicuous” privacy policies that contain at least 13 enumerated items of information about the company, its data processing, and the consumer’s rights under Privacy Shield. (For comparison, Safe Harbor only required four items to be disclosed in privacy notices.) In practice, this requires process mapping, gap assessments, and updates to privacy notices.
- (ii) Choice – Companies must give individuals an opt-out any time they intend to use data for a purpose that is “materially different” than the purposes for which the data was collected. Also, any time companies intend to transfer or use “sensitive data” for new and different purposes (e.g. data about race, ethnicity, medical conditions, religious beliefs, sex life), they must first obtain opt-in consent from users. Companies that implemented Choice principles under Safe Harbor should already have appropriate compliance infrastructure in place. For other companies, the Choice principle will require process-mapping to determine in-scope data, designate authorized uses, and gap-assess existing opt-out mechanisms.
- (iii) Enhanced Redress for Data Subjects – Privacy Shield requires companies to comply with numerous new dispute-resolution mechanisms:
- *First*, individuals are entitled to lodge a complaint directly with the company responsible for their data. The company must respond within 45 days.
 - *Second*, companies are obligated to designate and cooperate with an “independent recourse mechanism” (basically a mediation provider). Companies must inform consumers of who the mediation provider is, and ensure that consumers can lodge complaints (and participate in mediation) free of charge.

- *Third*, individual EU citizens can lodge complaints against Privacy Shield companies directly with their local DPA. The DPA will forward complaints to the DOC, which will investigate them at no cost to the individual.
- *Lastly* – and only after attempting all three of the above mechanisms – individuals can invoke a special Privacy-Shield-specific arbitration procedure. Privacy Shield companies are bound by the results of the arbitration.
- *Alternatively*, US companies can elect to work directly with European DPAs in resolving consumer complaints. If they do, they are bound by the decisions of a pan-EU panel established by DPAs to resolve consumer complaints. They must also inform both consumers and the FTC/DOT that complaints against them can be lodged with European DPAs.

(iv) Onward C2C Transfers – In order to transfer data to a another company acting as a controller, Privacy Shield requires companies to:

- Inform individuals about the “type or identity” of the data recipient and the purposes of the transfer;
- Give individuals an opportunity to opt out of the transfer; and
- Enter a written agreement with the recipient obligating it to (i) process data only for limited and specific purposes consistent with the consent provided by the individual, and (ii) maintain “the same level of protection” as required by Privacy Shield.
- Practically, this will require companies to map their transfers so they can gap-assess privacy notices and make sure opt-outs for in-scope data flows are in place. Also,

companies may need to negotiate addenda to existing contracts to bring contractual relationships into compliance.

(v) C2P Transfers and Vendor Management – Privacy Shield requires written contracts as the basis for any relationship with a processor. This will generally require businesses to engage in a contract and/or vendor management program for outsourced processing activities. As part of managing contractual relationships, Privacy Shield requires both due diligence as well as auditing of vendors. Notably, Privacy Shield contains a new liability rule ensuring that its Principles flow through to vendors: Privacy Shield Organizations are presumed liable for any violation of the Privacy Shield Principles committed by their vendors.

(vi) Verification – While Safe Harbor gave companies the option of conducting compliance audits, Privacy Shield now mandates that organizations annually verify that they are in compliance with Privacy Shield Principles, and that their published privacy policies are true. Privacy Shield permits organizations to do so through (a) self-assessment or (b) third-party audits. If self-assessing, an officer's signed certification will be required, and can be demanded by the FTC or DOT at any time.

(vii) Ongoing Obligations: Any organization that receives personal data under Privacy Shield must apply the Privacy Shield Principles to that information for as long as the organization retains it—even if the organization stops participating in (or is removed from) the Privacy Shield program. Note, however, that there is a significant chance the Commission may insert a Data Retention Principle into its final Privacy Shield decision that would require organizations to delete EU data after a specified time. Either way,

organizations will need to map their data flows and implement compliance systems for Privacy Shield data.

d. Privacy Shield Enforcement

Safe Harbor suffered under the criticism that it was a “check-the-box” system without real teeth. Privacy Shield aims to strengthen enforcement. In that regard both the FTC and the DOT have committed to proactively looking for false claims that an organization is a self-certified participant. Individuals and DPAs can also submit complaints regarding Privacy Shield participation.

Note that Privacy Shield provides that the DOT can demand an organization to “provide [all] information relating to the Privacy Shield” in its possession. Although this provision has not yet been tested in court, its terms imply that DOT’s commitment to conduct compliance reviews is supported by an ability to demand all (presumably non-privileged) Privacy-Shield-related information from an organization at any time.

Depending on the compliance violation at issue, different penalties could result ranging from removal from the privacy shield to enforcement action. In a removal from the Privacy Shield the companies need to return or destroy all personal data collected under the Privacy Shield, and they will be publicly shamed through a DOT list of organizations removed from Privacy Shield and an FTC list of Privacy Shield cases. An organization can also find itself subject to a DOT or FTC investigation or enforcement proceeding, including a cease-and-desist order or a judicial injunction. Such violations can be penalized at up to \$16,000 per violation or per day (for ongoing violations).

There is still a considerable chance that Privacy Shield will be challenged in the EU courts, most likely on grounds that transfers to the U.S. are still subject to—as Schrems and the Article 29 Working Party have put it—“mass and indiscriminate surveillance” by U.S. national-security agencies. The ECJ has become progressively stricter in interpreting fundamental privacy rights, not only in Schrems but in a series of other recent cases. The Article 29 Working Party has expressed serious reservations about the Privacy Shield, with some DPAs going further and suggesting that other transfer mechanisms such as model contracts appear to lack adequacy for data transfers to the United States. Companies may wish to seriously consider using Privacy Shield as the basis for their international transfers, especially because the ECJ made clear in Schrems that only it can overrule a Commission adequacy finding, and not an individual DPA.

e. First Annual Review of the EU-US Privacy Shield

The Privacy Shield is reviewed annually to ensure that it still provides an adequate level of protection for personal data. The Commission prepared the report on the first Privacy Shield annual review in October 2017.³⁰

In its annual review, the Commission noted that the US has introduced elements in the Privacy Shield, for instance a streamlined process to receive and review applications from companies that wish to certify, questionnaires as a tool to monitor companies’ effective compliance, and instruments to ensure smooth cooperation between enforcement authorities on both sides of the Atlantic. Further, the US Department of State has taken measures to ensure that the Ombudsperson mechanism is fully functional and ready to receive and address complaints.

³⁰ Report from the Commission to the European Parliament and The Council on the first annual review of the functioning of the EU-US Privacy Shield, SWD(2017) 344 final, p. 2-7

However, the Privacy Shield needs to be improved on a number of factors. The Commission recommended a number of key improvements in the field of general privacy and national security, including that:

- Companies should not be allowed to publicly announce that they are Privacy Shield-certified until the Department of Commerce has finalized the certification;
- The Department of Commerce conducts regular searches for companies falsely claiming participation in the Privacy Shield and conducts regular compliance checks, whereas it works together with Data Protection Authorities to develop guidance on the legal interpretation of Privacy Shield concepts (e.g. accountability) and to raise awareness (e.g. inform individuals about their rights);
- The U.S. administration swiftly appoints a permanent Privacy Shield Ombudsperson, as well as the missing members of the Privacy and Civil Liberties Oversight Board (PCLOB);

In both the commercial and national security areas, the Commission also called on the U.S. authorities to proactively fulfil their commitment to provide timely and comprehensive information about any development that could raise questions about the functioning of the Privacy Shield. On the whole, the report showed that the Privacy Shield continues to ensure an adequate level of data protection. However, there is room for improvement. At the time of writing of this chapter, the results of the second annual review have not yet been published.

The WP29 also published the results of its first review of the EU-US Privacy Shield in December 2017.³¹ Being quite more critical than the Commission, the WP29 identified several “significant concerns”. Albeit an improvement compared to the safe harbor, the WP29 called

³¹ Article 29 Working Party, WP255, EU-US Privacy Shield- First annual Joint Review, p. 3-7.

for significant improvement on a number of items including: lack of guidance for companies participating in Privacy Shield which leads to confusion regarding the companies' actual obligations; defining HR data too narrowly which restricts their protection; insufficient oversight and supervision regarding compliance and monitoring; an inconsistent approach on onward transfers from the EU to the US; lack of rules regarding automated decision making; insufficient evidence that US intelligent activities are tailored; and insufficient access to redress.

The WP29 has indicated that all the concerns above must be resolved before the second Privacy Shield review (expected in November 2018) otherwise it has threatened to bring claims regarding the Privacy Shield Adequacy decision before EU national courts. This may create additional uncertainty particularly since the Standard Contractual Clauses are currently being challenged before the Court of Justice of the European Union, following the referral of *Schrems II* by the Irish courts.

II. Transfers on the Basis of “Appropriate Safeguards”

When the Data Protection Directive was passed in 1995, it anticipated that many countries would not have the benefit of an adequacy decision. For such situations, it introduced the possibility of basing data transfers to non-EU countries on what came to be termed “appropriate safeguards” for individuals.³² “Appropriate safeguards” referred to legally binding commitments by companies to provide adequate protection over individuals' data, backed up by effective legal remedies for both affected individuals and European DPAs.

³² See Article 26(2) of the Directive and article 46(1) of the GDPR.

In data-protection literature, these transfer mechanisms are often referred to as “alternative transfer tools” or “alternative transfer mechanisms”—an allusion to the fact that while a Commission adequacy decision may represent the ideal basis for international data transfers, “appropriate safeguards” remain as alternatives for companies in countries where no adequacy decision exists.

Under the Directive, two primary “appropriate safeguard” mechanisms developed for permitting transatlantic data transfers are model contractual clauses (“Model Clauses”) and Binding Corporate Rules (“BCRs”). The GDPR expressly recognizes and permits both of these mechanisms.³³ Additionally, the GDPR creates new transfer mechanisms in the form of approved codes of conduct and certifications.³⁴

In the following, we will briefly sketch each alternative transfer mechanism, as well as address some of the practical considerations associated with implementing them under the GDPR.

1. Model Clauses

Model Clauses have proven particularly useful for companies that engage in large and routine transfers of data from the EU to the U.S. Many large and recognizable U.S. companies use Model Clauses as the basis of data flows from customers and subsidiaries because they are standardized and (by law) non-negotiable, which make them advantageous for standard terms as well as for intra-corporate arms-length agreements.

³³ See Article 46(2) of the GDPR.

³⁴ See Article 46(2)(e) of the GDPR.

Like the Directive, the GDPR continues to permit transfers on the basis of Model Clauses. To use the GDPR's language, "standard data protection clauses adopted by the Commission" constitute "appropriate safeguards" that permit data transfers to non-EU countries even in the absence of an adequacy decision.³⁵ Moreover, the GDPR expressly provides that Model Clauses adopted under the Directive will continue in force under the GDPR until amended, replaced, or repealed.³⁶ Practically speaking, this means that companies that have Model Clauses in place that predate the GDPR can continue to rely on them in the GDPR era.

Importantly, the GDPR expands the possibilities for Model Clauses in the future. In addition to the Commission's already-existing Model Clauses, the GDPR now grants national DPAs the authority to adopt their own "standard data protection clauses."³⁷ To do so, DPAs must first present proposed model clauses to the Commission for approval. If the Commission approves, companies subject to that DPA's jurisdiction can take advantage of its model clauses as a basis for international data transfers. This ground may be useful for the development of Model Clauses which accommodate specific sectorial needs, such as the cloud, insurance, or travel sector.

On a helpful note, the GDPR codifies several practices that developed under the Directive among certain DPAs regarding Model Clauses. This ensures these practices will be available EU-wide and not merely in isolated jurisdictions:

³⁵ See Article 46(2)(c) GDPR; *see also* Art. 28(7) GDPR.

³⁶ See Article 46(5) GDPR.

³⁷ See Article 46(2)(d) GDPR.

(i) Building Model Clauses into a larger instrument (or set of instruments) – The mere fact that Model Clauses must be adopted in their entirety and without modification does not mean they are the *only* acceptable terms for data-transfer agreements. For example, the 2010 C2P Model Clauses provide that they do “not preclude the parties from adding clauses on business related issues” as long as additional terms do not “contradict” the mandatory model clauses.³⁸ Indeed, it has become common practice throughout the EU to build Model Contracts into a larger instrument. The GDPR now expressly recognizes this practice by stating that processing agreements—whether C2P or P2P—can be based “in whole *or in part*” on Model Clauses adopted by the Commission or by DPAs.³⁹

(ii) Adding additional safeguards to the Model Clauses – The GDPR expressly encourages companies to go beyond Model Clause requirements and agree to “additional safeguards” for data protection: “controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.”⁴⁰ To date, some jurisdictions (such as France) already permitted this practice; the GDPR now officially recognizes it. The only requirements for such additional safeguards are that they cannot (a) contradict mandatory Model Clauses or (b) prejudice individuals’ privacy rights. In practice, additional safeguards are unlikely to run into such obstacles; for example, agreeing to encrypt data transfers would *strengthen* individuals’ privacy rights, and does not affect 2004 or 2010 Model Clauses.

(iii) Model P2P Contracts – To date, the Commission has adopted only controller-to-controller and controller-to-processor Model Clauses—but no Model Clauses for processor-to-

³⁸ See Commission Decision 2010/87/EC, Annex cl. 10.

³⁹ See Article 28(6) GDPR.

⁴⁰ See Recital 109 GDPR.

processor (P2P) contracts. Although model P2P clauses have long been discussed in the EU and WP29 even went so far as to draft (but not finalize) such clauses, model P2P clauses are presently a rarity in the EU.⁴¹ The GDPR permits both the Commission as well as national DPAs to adopt model P2P clauses.⁴²

(iv) Ad Hoc Contracts – Finally, the GDPR allows companies to draft ad hoc data transfer agreements and submit those for approval to the competent DPA.⁴³ These can also be processor-to-processor clauses. It is expected that most DPAs would require that the provisions of the Model Clauses are largely reflected in these ad hoc agreements (even if that is not a formal requirement).

Furthermore, the GDPR simplifies the formalities for international transfers by abolishing notification and authorization requirements that are in force in some jurisdictions (e.g. France, Spain, Austria, Denmark, Greece, etc.). The GDPR clarifies that transfers on the basis of Model Clauses do not require any “specific authorization” by a DPA.⁴⁴

a. Next Steps and Practical Expectations

Like adequacy decisions, the GDPR requires the Commission to periodically review the Model Clauses it has approved.⁴⁵ *Schrems*’ requirement that EU data receive not just adequate, but “essentially equivalent” protection in foreign legal systems may induce the Commission to review and upgrade the 2004 and 2010 Model Clauses. Further the ongoing *Schrems II* case

⁴¹ Spain is one rare country that has produced its own P2P Model Clauses.

⁴² See Article 46(5)-(6), Recital 168 GDPR.

⁴³ See Article 46 (3)(a).

⁴⁴ See Article 46(2) GDPR.

⁴⁵ See Recital 106 GDPR.

that attempts to invalidate model clauses as an adequate transfer mechanism adds uncertainty as to whether they will be a trusted mechanism in the future. In essence, Mr. Schrems renewed and reformulated his original complaint, alleging that Facebook's specific contracts (Facebook relies on model contracts to transfer data from the EU to the US) did not meet the obligations of EU law and that, in any case, the contracts could not provide adequate protection where national laws of the third country would override them. The current model clauses have an inbuilt emergency clause whereby data flows can be terminated by the relevant local data protection authority, (in this case the Irish DPC), whenever there is a conflicting law in a foreign country. In his submissions, Mr Schrems mirrors the position in the 2015 case, stating that US surveillance laws and practices (brought to light by the Snowden leaks) are incompatible with EU law, and therefore any company party to such laws should have their data flows suspended.⁴⁶

The Irish High Court referred the case to the Court of Justice of the European Union. In its decision, the High Court concurred with the submission of the Irish DPC ruling that a targeted approach to Facebook alone did not go far enough to tackle the issue. The Court contended that there were deeper, systematic issues at the heart of the model clauses framework as a whole, and because of the EU wide implications of these issues it is appropriate to refer the case to the Court of Justice.

At the writing of this paper the case is ongoing. If the Court of Justice were to invalidate the model clauses it would cause significant distress to thousands of companies that rely on them to transfer data from the EU to the US on a daily basis. At the same time, this may turn out to

⁴⁶ Blogpost, White and Black, Standard Contractual Clauses At Risk After Schrems II Decision, available at : <https://www.wablegal.com/standard-contractual-clauses-risk-schrems-ii-decision/>

be a legally moot battle as it addresses decisions under the expired Data Protection Directive and the GDPR allows data protection authorities and the Commission to fashion such model clauses. This could, hence, potentially be an easy hurdle to avoid.

2. Binding Corporate Rules (“BCRs”)

BCRs refer to an intra-company code of conduct that sets forth principles and rules which apply to the processing of personal data—including cross-border transfers—within a company group.

a. BCRs under the Directive

BCRs have been developed as an alternative transfer mechanism under the Directive. In 2003 and 2005, WP29 publicly endorsed BCRs as valid bases for international data transfers.⁴⁷

BCRs proved to be a useful mechanism for organizations with complex international structures – instead of having to justify international transfers on a transfer-by-transfer (or client-by-client) basis, they could simply present one single set of transfer rules to DPAs for approval. This prevented having to conclude Model Contracts with potentially thousands of European suppliers or clients.

The downside of BCRs under the Directive’s regime was that companies had to obtain BCR approval in a substantial number of European jurisdiction from which they transferred data to

⁴⁷ See WP29 Working Document of June 3, 2003 on Transfers of personal data to third countries: applying article 26 (2) of the EU data protection Directive to Binding Corporate Rules for international data transfers, (WP 74); WP29 Working Document of April 14, 2005 Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules" (WP 107).

the U.S. In some countries, export permits are required for specific data streams (rather than having all data streams that take place under the BCR authorized).

b. BCRs under the GDPR

In contrast to the Directive, the GDPR expressly recognizes BCRs as a legal basis for the transfer of personal data within a group of companies. In addition, groups of enterprises that are engaged in a joint economic activity may also apply for a BCR. The GDPR does not give specific examples of the types of scenarios that are in scope here, however, one can think of airline companies cooperating in a loyalty program, or joint venture companies.⁴⁸ Another novelty is that companies will no longer need to apply for data transfer permits based on BCRs. These have been explicitly abolished, which is positive and will likely catalyze BCR applications.⁴⁹

The GDPR contains several important changes to existing BCR practices that make them a much more attractive option for businesses. At present, BCRs are generally reserved to data controllers. The GDPR, however, opens the possibility for *processors* to establish their own BCRs (generally referred to as “BCR-Ps”).⁵⁰ This was a hotly-debated topic during the GDPR’s drafting, and BCR-Ps survived and made it into the GDPR’s final provisions. It can be anticipated that processors will increasingly rely on BCR-Ps to justify transfers to the US because once BCR-Ps are in place, processors can engage in practically unlimited data transfers to their US co-entities.

⁴⁸ See Article 47 of the GDPR.

⁴⁹ See Article 46(2)(b) GDPR.

⁵⁰ See Article 47(3) GDPR.

Further, the GDPR grants the Commission authority to “specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities” for BCRs.⁵¹ This could lead to a set of “Model BCR” provisions or model BCR approval procedures which, if adopted, would be binding on DPAs and further streamline the BCR approval process.

What changes for Controller BCRs

Recent guidance from the WP29 has streamlined the elements and principles required to be found in Binding Corporate Rules through a table that companies can easily access. These new elements may require companies to update their BCRs so that they remain compliant with the GDPR.⁵²

In this regard the WP29 highlighted the following elements:

- *Right to lodge a complaint*: Data subjects should be given the choice to bring their claim either before a competent DPA or before the competent court of the EU Member States;
- *Transparency*: All data subjects must have adequate information⁵³ regarding their rights and the means to exercise said rights;
- *Scope of application*: The BCRs must specify the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity and of each of its members.⁵⁴ The BCRs must also specify its material scope, for instance the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the

⁵¹ See Article 47(3) GDPR.

⁵² WP256 Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, 29 November 2017

⁵³ See Articles 13 and 14 GDPR

⁵⁴ See GDPR Article 47(2)(a)

types of data subjects affected and the identification of the recipients in the third country or countries.⁵⁵

- *Data Protection principles*: Along with the principles of transparency, fairness, purpose limitation, data quality, security, the BCRs should also explain the other principles referred to in Article 47.2.d – such as, in particular, the principles of lawfulness, data minimisation, limited storage periods, guarantees when processing special categories of personal data, the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
- *Accountability*: Every entity acting as data controller shall be responsible for and able to demonstrate compliance with the BCRs;⁵⁶
- *Third country legislation*: The BCRs should have a commitment whereby if a member of the group of enterprises is subject to third country laws that may have a substantial adverse effect on the guaranteed provided by the BCRs, this will be reported to the competent supervisory authority (e.g. legally binding request for disclosure of personal data by a law enforcement authority or state security body).

While the BCR authorizations made on the basis of Article 26(2) of Directive 95/46/EC will remain valid, the WP29 recommends that BCR approved companies update their BCRs for GDPR purposes.

What changes for Processor BCRs

The WP29 also issued recent guidance on Processor BCRs and highlighted the following changes:

⁵⁵ See GDPR Article 47(2)b

⁵⁶ See GDPR Article 5(2)

- *Scope of application*: Same as for Controller BCRs.
- *Third party beneficiary rights*: Data subjects should be able to enforce the BCRs as third party beneficiaries directly against the processor where the requirements at stake are specifically directed to processors in accordance with the GDPR.⁵⁷
- *Right to lodge a complaint*: Same as for Controller BCRs.
- *Data Protection principles*: Along with the obligations arising from principles of transparency, fairness, lawfulness, purpose limitation, data quality, security, the BCRs should also explain how other requirements, such as, in particular, in relation to data subjects rights, sub-processing and onward transfers to entities not bound by the BCRs will be observed by the processor;
- *Accountability*: Processors will have an obligation to make available to the controller all information necessary to demonstrate compliance with their obligations including through audits and inspections conducted by the Controller or an auditor mandated by the Controller;⁵⁸
- *Service Agreement*: The Service Agreement between the Controller and the Processor must contain all required elements as provided by Article 28 of the GDPR.

Exactly like it did with Controller BCRs, the WP29 has endorsed the Processor BCR approved companies to update their BCRs for GDPR purposes.

3. Codes of Conduct and Certifications

⁵⁷ See Articles 28, 29, 79 GDPR

⁵⁸ See Article 28(3)(h) GDPR

The GDPR contains new options for companies to transfer data in the form of (i) a code of conduct approved by a DPA and/or the EU Commission⁵⁹, and (ii) a certification mechanism such as a privacy seal or mark, issued by an approved certification body⁶⁰. Controllers or processors in non-EU countries can commit to comply with these mechanisms in order to provide “adequate safeguards” permitting them to receive data transfers from the EU. The GDPR encourages the use of both mechanisms.⁶¹

a. Codes of Conduct

The Data Protection Directive permitted Codes of Conduct as a basis for justifying processing—but not as a basis for permitting international data transfers. The GDPR now expressly declares that Codes of Conduct, if properly approved, can serve as a basis for international data transfers because they provide “adequate safeguards” for EU data abroad.

Codes of Conduct are a co-regulatory instrument drawn up by “associations and other bodies” representing categories of companies. To be considered an “adequate safeguard” permitting international transfers under the GDPR, they must (a) set forth rules that ensure equivalent protection of EU data abroad, and (b) be coupled with a mechanism whereby they are made legally binding on companies that commit to comply with them (*e.g.* via a contract between EU controller and US processor agreeing to implement an approved Code of Conduct).⁶²

The approval of Codes of Conduct proceeds as follows:

⁵⁹ See Articles 40(2)(i) & 46(2)(e) GDPR.

⁶⁰ See Article 46(2)(f) GDPR.

⁶¹ See Article 57(m) & (n) GDPR.

⁶² See Article 44(2)(e) GDPR.

- The association drafting the Code of Conduct must present it to the DPA having jurisdiction over the international transfers the Code seeks to legitimate.⁶³ If the draft Code of Conduct relates to processing in only one member state, the DPA may proceed to approve the Code.⁶⁴
- If, however, the draft Code relates to processing in multiple EU member states (and most probably will), the DPA must first forward the draft Code to the European Data Protection Board.⁶⁵
- The Board will issue an opinion determining whether the draft Code of Conduct provides “appropriate safeguards” for international transfers.⁶⁶ If the Board finds the Code does provide adequate safeguards, the DPA may proceed to approve it.

Moreover, if the Board determines a draft Code of Conduct provides “adequate safeguards” for transfers, it must forward its opinion to the Commission.⁶⁷ The Commission then has the opportunity to determine whether the draft Code of Conduct has “general validity” throughout the EU. Such would then be determined by a Commission Decision.⁶⁸

In keeping with the co-regulatory character of Codes of Conduct, primary compliance monitoring is *not* carried out by DPAs, but by independent “bodies” that have been DPA-

⁶³ See Article 40(5) GDPR.

⁶⁴ See Article 40(6) GDPR.

⁶⁵ See Article 40(7) GDPR.

⁶⁶ See Article 40(7) GDPR.

⁶⁷ See Article 40(8) GDPR.

⁶⁸ See Article 40(9) GDPR.

accredited.⁶⁹ These independent compliance monitoring organizations are empowered to take any “appropriate action” against companies who violate the Code of Conduct,⁷⁰ although the universe of permissible enforcement actions in the absence of DPA involvement would likely be regulated some degree by the Code of Conduct itself. Third-party enforcement could be either a net plus or a net minus for businesses. On the one hand, third-party compliance monitoring organizations could be more amicable to work with than DPAs. On the other hand, however, they may not be – and sector-specific monitoring organizations may have more relevant technical expertise and a much smaller case load than a typical DPA.

The benefits of the Codes of Conduct include that a particular sector follows the GDPR requirements for data protection, addresses the level of risk and creates effective safeguards to mitigate it, is transparent and accountable, improves standards by establishing best practice and is committed to international transfers. It also provides a competitive advantage for companies in that sector and helps towards a strong brand recognition particularly in times where being privacy friendly is a strong marketing tool.

Even though Codes of Conduct existed under the previous regime, they have a more prominent position under the GDPR. As of the time of writing of this piece there is no Code of Conduct that has been approved post-GDPR, however it is expected that sectors will actively pursue this in the near future.

b. Certifications

⁶⁹ See Article 41(1) GDPR.

⁷⁰ See Article 41(4) GDPR.

Certifications – which typically take the form of a privacy mark or seal – are a new transfer mechanism the GDPR introduces. A company in a non-EU country can apply for and receive a certification or seal indicating it offers appropriate protection to EU data. If it combines this certification with a legally binding commitment to apply the certification standards, it will be considered to provide “adequate safeguards” and thus receive data transfers from the EU.⁷¹

Certifications can only be issued to companies by DPAs or by approved “certification bodies.” Organizations can be accredited as GDPR ‘certification bodies’ if they meet requirements set by their local DPA; however, if a body intends to issue certifications that affect processing in more than one member state, the DPAs of those member states can involve themselves in the accreditation-standard-setting process and make approval by the European Data Protection Board necessary.⁷² In the end, either the Board or a local DPA will set the standards for organizations to be accredited as a certification body. Once applicable accreditation standards are set, the actual accreditation as a “certification body” will be conducted by an organization’s local DPA.

U.S. companies seeking to obtain a certification must apply to either an appropriate DPA or to an accredited certification body.⁷³ The criteria for issuing certifications may be set by the certification body’s local DPA—however, again, if certifications will relate to processing in more than one member state, other DPAs may escalate the certification-criteria-setting process to the Board for final resolution. Once certification criteria have been set, they will be applied by accredited certification bodies and DPAs upon applications for certifications by companies.

⁷¹ See Article 46(2)(f) GDPR.

⁷² See Articles 43(3) GDPR.

⁷³ See Article 42(5) GDPR.

In examining whether to issue a certification to a U.S. company, accredited certification bodies and DPAs can demand “all information and access to processing activities which are necessary to conduct the certification procedure”—and companies must comply.⁷⁴ Note that if the Board approves of a set of certification criteria, these criteria are eligible for EU-wide use as a European Data Protection Seal.⁷⁵

Once issued, certifications are valid for a maximum of three years. However, accredited certification bodies are empowered and required to continually monitor compliance, receive individual complaints, and withdraw certifications as appropriate.⁷⁶ As in the case of Codes of Conduct, it is difficult to predict whether working with a third-party certification body (as opposed to a DPA) will be more or less advantageous for businesses.

Moving forward, certifications are the newest and most untested of the “appropriate safeguards” available under the GDPR. There at present no accredited certification providers, nor are accreditation standards set yet. The WP29 recently issued draft guidelines on the accreditation of certification bodies under the GDPR.⁷⁷ There the WP29 recognizes that meaningful certification mechanisms can improve compliance with the GDPR and transparency for data subjects in B2B relations, for example between controllers and processors. The guidelines provide some high-level guidance as to how Member States, supervisory authorities and national accreditation bodies can interpret and implement the provisions related to certification and create a harmonized baseline. It remains to be seen how this will be implemented in practice.

⁷⁴ See Article 42(6) GDPR.

⁷⁵ See Article 42(5) GDPR.

⁷⁶ See Articles 42(7), 43(2)(d) GDPR.

⁷⁷ WP261, Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679

III. Derogations

The Directive established an exclusive list of seven limited exceptions (or “derogations”) to the general prohibition on transferring data outside the EU.⁷⁸ The GDPR adopts the same list but adjusts the requirements for claiming derogations in some cases.⁷⁹ Further the WP29 recently published guidelines on how these derogations should be used and interpreted.⁸⁰

Traditionally, reliance on a derogation has not always been favored by DPAs, especially for massive or systematic transfers of personal data. The GDPR codifies this practice by making clear that reliance on derogations is its last choice among transfer mechanisms and only available in limited circumstances. Companies may only base international transfers if (a) no adequacy decision is present, and (b) none of the “appropriate safeguards” discussed above are available (such as Model Clauses, BCRs, Codes of Conduct, or certifications).⁸¹

Therefore, derogations under Article 49 GDPR are exemptions from the general principle that personal data can only be transferred to third countries if an adequate level of protection is provided in the third country or if appropriate safeguards have been adduced and the data subjects enjoy enforceable and effective rights. This means that derogations must be interpreted restrictively so that the exception does not become the rule.

⁷⁸ See Article 26(1) Directive.

⁷⁹ See Article 49 GDPR.

⁸⁰ WP261, Guidelines on Article 49 of Regulation 2016/679, Adopted on 6 February 2018

⁸¹ See Article 49(1) GDPR.

The WP29 makes a particular reference to the GDPR wording, namely the term “occasional” in recital 111 and the term “not repetitive” for compelling legitimate interests.⁸² These terms indicate that transfers may happen more than once, but not regularly, and would occur outside the regular course of actions, for instance under random unknown circumstances and within arbitrary time intervals (e.g. a stable relationship between two companies that exchange data is systematic so they cannot rely on derogations).

However, even the derogations that are not expressly limited as “occasional” or “not repetitive” have to be interpreted in a way which does not contradict the very nature of the derogations as the exceptions from the rule. In any event, every derogation must pass the necessity test, meaning the evaluation of whether a transfer of personal data can be considered necessary for the specific purposes that the derogations try to achieve.

The GDPR also introduces a new provision in Article 48 that must be taken into account when considering transfers of personal data. In particular, the GDPR provides that decisions from third country authorities, courts or tribunals are not in themselves legitimate grounds for data transfers to third countries. Hence, a transfer in response to a decision from third country authorities is only lawful if in line with the other conditions set out in Chapter V regarding cross-border data transfers. In situations where there is an international agreement (e.g. a mutual legal assistance treaty), EU companies are expected to refuse direct requests and refer such requests to the existing treaty.

The GDPR’s derogations permitting international transfers are as follows:

⁸² See Article 49 (1)(2)

1. Consent

Consent was one of the classic legal bases for transfers under the Directive,⁸³ and the GDPR maintains consent as a transfer basis.⁸⁴ Traditionally, consent to an international transfer must be informed, freely given, and unambiguous.⁸⁵

In practice, consent has always been an uncertain basis for transfers, and it will become even more so under the GDPR. To start with, consent needs to be “freely given”. Companies have always had trouble showing that consent is freely given. Employee consents are always subject to attack before DPAs due to the relationship of dependency between employees and employer. Moreover, if companies make purchasing goods or services dependent on consenting to international data transfers—*e.g.* by not letting customers purchase until they click a box consenting to privacy policies with baked-in transfers—the GDPR strongly suggests this is an impermissible ‘tying arrangement’ that invalidates consent as unfreely given.⁸⁶

Further, even if individuals provide consent, they may revoke their consent at any time. In fact, the GDPR requires companies to (a) make revoking consent as easy as giving it⁸⁷ and (b) affirmatively inform individuals about their right to withdraw consent.⁸⁸

Finally, consent has always had to be “informed,” but the information necessary to meet this obligation was not defined. The GDPR now expressly clarifies that informed consent requires

⁸³ See Article 26(1)(a) Directive.

⁸⁴ See Article 49(1)(a) GDPR.

⁸⁵ See Article 26(1)(a) Directive; Article 7 GDPR.

⁸⁶ See Article 7(4) GDPR.

⁸⁷ See Article 7(3) GDPR.

⁸⁸ See Article 14(2)(d) GDPR.

companies to specifically inform individuals of “the possible risks of [international] transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.”⁸⁹

All these conditions make consent a risky choice for companies to invoke in order to legitimize cross-border data transfers.

2. Other Derogations

The GDPR retains other derogations which are similar to the derogations under the Directive.

This includes:

- (i) Contract Performance: Transfers which are necessary for the performance of a contract between the data subject and the controller.⁹⁰ The classic example of a data transfer on this basis is a hotel chain sending customer data to the US to book an EU customer’s room in New York. This derogation also permits data transfers necessary to implement pre-contractual measures requested by the data subject (*e.g.* AirBnB transferring customer data to a Brazilian host as part of a request for information about an apartment before booking).
- (ii) Third-Party Contracts in the Individual’s Interest: Transfers which are necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person (*e.g.* data

⁸⁹ See Article 49(1)(a) GDPR.

⁹⁰ See Article 49(1)(b) of the GDPR, similar to article 26(1)(b) of the Directive.

transferred from an EU citizen to a US company to prepare his/her contract of employment so that they relocate to the US).⁹¹

- (iii) Public Interest: Transfers necessary for important reasons of public interest.⁹² This derogation will likely not be claimable by private entities, especially since the public interest claimed as the basis for the transfer must be “recognized in Union law or in the law of the Member State to which the controller is subject.”⁹³
- (iv) Legal Claims: Transfers necessary for the establishment, exercise or defense of legal claims.⁹⁴
- (v) Danger to Life & Limb: Transfers necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent⁹⁵; or
- (vi) Transfers from EU Public Registries: Transfers made from a register which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.⁹⁶

3. A New Ground: “Compelling Legitimate Interests” of the Controller

⁹¹ See Article 49(1)(c) of the GDPR, similar to article 26(1)(c) of the Directive.

⁹² See Article 49(1)(d) of the GDPR, partly similar to first part of article 26(1)(d) of the Directive

⁹³ See Article 49(4) GDPR.

⁹⁴ See Article 49(1)(e) of the GDPR, similar to second part of article 26(1)(d) of the Directive.

⁹⁵ See Article 49(1)(f) of the GDPR, similar to article 26(1)(e) of the Directive.

⁹⁶ See Article 49(1)(g) of the GDPR, similar to article 26(1)(f) of the Directive.

The difficulty of complying with the requirements of consent – and the narrowness of the other derogations – often causes companies to look for alternative grounds for international transfers. The GDPR creates a new option to transfer personal data abroad based on “compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject.”⁹⁷

Traditionally, the notion of a controller’s “legitimate interests” was broad, and the GDPR lists examples of potential legitimate interests such as fraud prevention, information security, and intra-group disclosures.⁹⁸ However, the conditions for basing a transfer on the GDPR’s new legitimate-interest derogation are *very* restrictive.

In particular, only data controllers may rely on this derogation and they need to prove that no other data transfer ground can be available, including the other derogations, whereas the transfer(s) at issue must not repetitive and involve only a limited number of data subjects.⁹⁹

This implies that the data exporter can demonstrate serious attempts in this regard, taking into account the circumstances of the data transfer. This may for example and depending on the case, include demonstrating verification of whether the data transfer can be performed on the basis of the data subjects’ explicit consent to the transfer under Article 49 (1) (a). However, in some circumstances the use of other tools might not be practically possible. For example, some types of appropriate safeguards pursuant to Article 46 may not be a realistic option for a data exporter that is a small or medium-sized company. This may also be the case for example, where the data importer has expressly refused to enter into a data transfer contract on the basis

⁹⁷ See Article 49(1)(h)

⁹⁸ See Recital 47 of the GDPR.

⁹⁹ *Idem*.

of standard data protection clauses (Article 46 (2) (c)) and no other option is available (including, depending on the case, the choice of a different “data importer”).

Further, the controller must have assessed all the circumstances surrounding the data transfer and based on this assessment adduced suitable safeguards.¹⁰⁰ In selecting privacy safeguards, the processor consider the nature of the data to be transferred, the purpose and duration of the proposed processing operations, and the situation in the destination country.¹⁰¹ Finally, the controller must notify the relevant DPA and all affected data subjects that it is relying on this derogation.¹⁰²

Especially in light of the necessary disclosures to all affected data subjects, companies should not expect to rely on the new “legitimate interest” transfer mechanism unless it is absolutely necessary.

IV. Penalties for Non-Compliance

Under the Directive, fines for non-compliance were limited to amounts set by national laws. These tended to be small by American standards, such as Germany’s fine regime which topped out at €300,000.

¹⁰⁰ *Idem.*

¹⁰¹ *See* Recital 113 of the GDPR.

¹⁰² *Idem.*

The GDPR dramatically increases the fines available for violations regarding international transfers. Transfer violations fall under the GDPR's harshest fine category and can be penalized by fines of up to €20 million or 4% of a company's worldwide annual turnover.¹⁰³

These fines rival the penalties available for antitrust violations, and place a premium on setting up transfer infrastructure now that the GDPR is in place.

V. Conclusion

The GDPR brought many welcome changes for businesses' data-transfer compliance programs. In general, international transfers involve far less red tape. Gone are the days of DPA notifications and permit applications, and in their place a number of safeguard-based mechanisms—often run not by DPAs, but by independent private third parties—should arise. Moreover, the GDPR contains numerous provisions through which processors can make regular, systematic, and massive international transfers GDPR-compliant.

Nonetheless, the GDPR ushers in changes that will require companies to do business differently in the future. Consent as a basis for international transfers will be very difficult to rely on, and doing so will carry the risk of €20 million fines. The same goes for all other derogations, which for the first time have been expressly disfavored by an EU legislative enactment.

These changes, along with the GDPR's new fine levels, will require companies to proactively manage their data-transfer programs, and to be attentive to any changes on the horizon. In this regard, the requirement that U.S. law offer "essentially equivalent" protection to EU data as

¹⁰³ See Article 83(5)(c) GDPR.

EU law will likely result in regular reviews of adequacy decisions and safeguard mechanisms. Companies will need to pay attention to and flexibly anticipate the results of these reviews.

In total, however, the GDPR provides numerous avenues for companies with transatlantic data flows to keep those flows flowing, and to do so with substantially less bureaucracy than before. If managed correctly, transfer compliance under the GDPR can work strongly to companies' advantage.