TRANSFERRING DATA FROM THE EU:
PRIVACY SHIELD AND DATA TRANSFERS UNDER THE GDPR

On May 25, 2018, the EU's new General Data Protection Regulation (GDPR) will enter into force. One of the questions at the top of most companies' agendas is what effect the GDPR will have on their transatlantic data flows. Every day, companies transfer data from the EU to the U.S. to manage their IT systems, comply with regular reporting obligations, centralize HR data, exchange customer files, make data storage efficient through shared systems, and migrate IT into the cloud.

Despite the ubiquity and mass of transatlantic data transfers, many companies are often surprised to learn that EU law generally *prohibits* transfers of data to countries outside the EU. Ever since the EU Data Protection Directive (the "Directive") was passed in 1995, data transfers to non-EU countries are only permitted when personal data will receive an "adequate level of protection" upon arrival in the destination country.

The General Data Protection Regulation (GDPR) [1] adopts this same framework: transfers to non-EU countries are generally prohibited unless data can expect an "adequate level of protection" abroad. Both the Directive and the GDPR provide various mechanisms for permitting transfers to the U.S., including:

1. An "adequacy decision" by the European Commission.
2. EU-sanctioned "appropriate safeguards" for transfers such as model clauses.
3. Statutory exceptions to the general transfer prohibition, such as consent or contractual obligations.

Additionally, the GDPR contains new transfer mechanisms such as (4) certifications and (5) approved codes of conduct. Furthermore, the GDPR also formalizes binding corporate rules (BCRs) as a legal basis for international data transfers. The GDPR also puts an end to prior-notification and authorization work, which constituted an administrative hassle for companies.

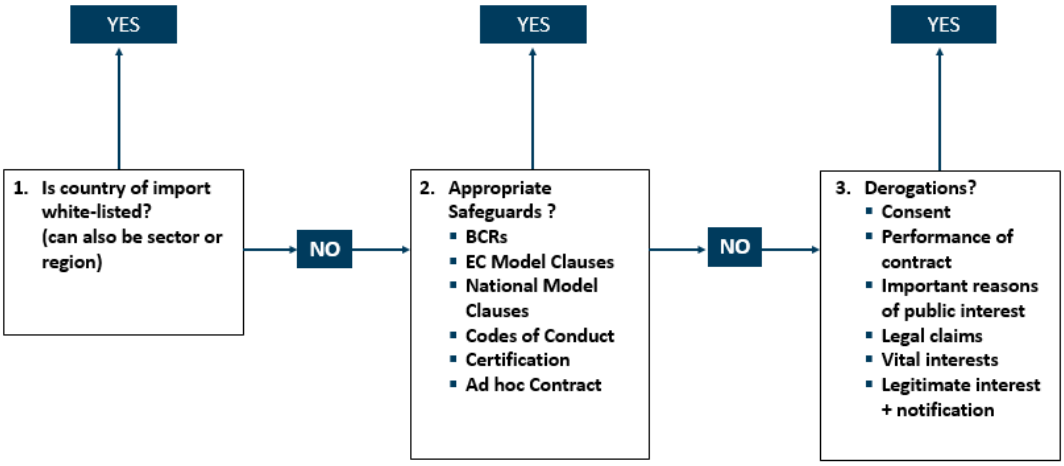
The GDPR establishes a clear hierarchy among its transfer mechanisms. Its ideal transfer mechanism is an adequacy decision issued by the Commission – in such a situation, one of the EU's three leading institutions has formally declared that the destination country for a data transfer offers adequate data protection (note that adequacy decisions can now also cover "a territory or one or more sectors within a third country").[2] 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, and

[1] Art. 25 Directive.

[2] Art. 45(1) GDPR.

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 article, we will assess the international transfer mechanisms available under the GDPR.[3] We will also show how these mechanisms can fit into a larger data-management strategy.

I. Adequacy Determinations of the EU Commission[4]

1. Transfers to Jurisdictions Offering "Adequate Level of Protection"

The European Commission has statutory authority to determine that a non-EU jurisdiction offers an "adequate level of protection" for personal data.[5] 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). An adequacy decision is binding for all EU member states and generally permits unlimited data transfers to the country the Commission has designated as "adequate."[6] Over time, the Commission's adequacy

[3] 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.

[4] Art. 45 GDPR.

[5] Art. 25(6) Directive & Art. 45 GDPR.

[6] Note, however, that an adequacy decision does not prevent national DPAs from receiving complaints from EU data subjects and, on the basis of those complaints, investigating whether transfers to the destination country are actually adequately protected in that specific case. *See Schrems v. Data Protection Commissioner*, Case C-362/14 at ¶¶ 40-66 (European Court of Justice [ECJ] October 6, 2015). Moreover, adequacy decisions usually contain provisions permitting DPAs to suspend transfers in certain extraordinary situations. For example, the Commission's adequacy decision for Canada provides that European DPAs may suspend data flows to Canadian recipients if (1) a competent Canadian DPA has determined that a Canadian company is breaching data-protection standards; or (2) there is a "substantial likelihood" that data-protection standards are not being observed, and "reasonable grounds" to believe that Canadian DPAs will not remedy the issue. *See* Commission Decision of 20

decisions have generated a "whitelist" of countries—such as Israel, Argentina, Switzerland, and Canada—to which companies can transfer personal data without limitation.[7]

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.[8] This means that sectoral data privacy legislation such as children's privacy laws or telecom privacy laws in a certain country may be declared adequate.

- The GDPR sets forth new minimum factors the Commission must consider when issuing an adequacy decision,[9] such as:
    - The destination country's statutes and case law on data protection, national security, and onward transfers.
    - Data subject rights in the destination country.
    - The existence (or lack thereof) of independent supervisory authorities in the destination country.
    - Any international commitments regarding data protection the destination country has entered into.

The onward transfer regime and potential access by the destination country's public-sector or national-security authorities are factors that clearly have more weight than the others and must be kept in mind when assessing transfer risks.

Under the GDPR, the Commission's adequacy decisions are dynamic. They must be reviewed periodically—at least every four years[10]—but the Commission is also obligated to monitor whitelisted countries "on an ongoing basis" to see if circumstances arise that would affect its

December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, 2002/2/EC, at Art. 3.

[7] To date, the Commission has whitelisted the following countries: Andorra (Decision 2010/625/EU); Argentina (Decision 2003/490/EC); Canada (Decision 2002/2/EC); Switzerland (Decision 2000/518/EC); Faeroe Islands (Decision 2010/146/EU); Guernsey (Decision 2003/821/EC); Israel (Decision 2011/61/EU); Isle of Man (Decision 2004/411/EC); Jersey (Decision 2008/393/EC); New Zealand (Decision 2013/65/EU); Uruguay (Decision 2012/484/EU).

[8] Art. 25(6) Directive.

[9] Art. 45(2) GDPR.

[10] Art. 45(3) GDPR.

adequacy decision.[11] The Commission retains full power to revoke an adequacy decision at any time after giving the affected jurisdiction notice and an opportunity to respond.[12]

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.[13] This means that the Commission's whitelist of permissible destination countries will remain valid 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 once the GDPR comes into effect on May 25, 2018.

Still, some legal uncertainty remains. Decisions of the European Court of Justice (ECJ) 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."[14] If the Commission comes to the conclusion that the GDPR results in a *higher* level of data protection than the Directive, that would mean that any adequacy decision would be reviewable to determine whether the country at issue provides data protection that is "essentially equivalent" to the higher GDPR standards.

Although it is unlikely the Commission will begin publicly questioning its own adequacy decisions as soon as the GDPR enters into force, it can be expected that whitelisted countries will come under more regular Commission review.

2. 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 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 more than 4,000 American companies relied on to legitimize their transatlantic data transfers. From its inception, however, some European DPAs consistently criticized Safe Harbor for not offering true "adequacy," especially for transfers to data processors and onward transfers. Following the Snowden revelations, Safe

[11] Art. 45(5) GDPR.

[12] *Id.*

[13] Art. 45(9) GDPR.

[14] Art. 45(4) GDPR.

Harbor fell under even more criticism as not providing sufficient protection against U.S. surveillance. In the landmark *Schrems* decision of October 6, 2015,[15] the ECJ invalidated Safe Harbor on the basis of surveillance concerns (albeit not formally). As a consequence, thousands of businesses rushed to identify alternatives to transfer personal data to the U.S., with most turning to EU model clauses.

b. Privacy Shield

The EU-U.S. Privacy Shield is under negotiation (as of May 2016) to replace Safe Harbor. In February 2016, the Commission, DOC, and Federal Trade Commission (FTC) released a 130-page package of Privacy Shield documents. Like Safe Harbor, Privacy Shield is a self-certification regime that would permit any company that self-certifies to abide by the Privacy Shield Principles to transfer personal data from the EU to the U.S.

The EU Commission published a draft adequacy decision on February 26, 2016,[16] tentatively finding that Privacy Shield results in an "adequate level" of data protection in the U.S. If adopted, the Commission's adequacy decision will again permit transatlantic data transfers in a manner similar to the approach under Safe Harbor. However, the Commission's adequacy decision is not final; at present, an influential advisory body of EU DPAs known as the Article 29 Working Party has published a formal opinion on the draft in which it lists concerns and requests clarification of central issues.[17] The Commission is expected to consider minor changes to its draft adequacy decision that address the Article 29 Working Party's concerns and to proceed with issuing a final adequacy decision as early as June 2016. (Once the final adequacy decision is issued, one can speak of Privacy Shield having been "adopted" by the EU.)

c. Privacy Shield Principles

Once Privacy Shield is adopted, companies that self-certify they will comply with the Privacy Shield Principles will be permitted to transfer EU data to the U.S. The Privacy Shield Principles are similar to the principles that existed under Safe Harbor:

- Notice
- Choice
- Accountability for Onward Transfer
- Security
- Data Integrity and Purpose Limitation

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

[16] Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council of the adequacy of the protection provided by the EU-U.S. Privacy Shield., February 26, 2016

[17] *See* WP29 Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision (WP 238), April 13, 2016. Also, the Commission's draft adequacy decision must be reviewed by the EU data protection supervisor and the EU member states prior to finalization.

- 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.

1) 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 will require process mapping, gap assessments, and updates to privacy notices.

2) 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, or 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 assess gaps in existing opt-out mechanisms.

3) 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 DPAs. 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*, U.S. 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/DOC that complaints against them can be lodged with European DPAs.

4) 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.
- Enter a written agreement with the recipient obligating it to (1) process data only for limited and specific purposes consistent with the consent provided by the individual; and (2) maintain "the same level of protection" required by Privacy Shield.

Practically, this will require companies to map their transfers so they can 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.

5) 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 and 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.

6) 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 accurate. Privacy Shield permits organizations to do so through self-assessment or third-party audits. If self-assessing, an officer's signed certification will be required and can be demanded by the FTC or DOC at any time.

7) 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 as described below:

1) False Participation Reviews – Both the FTC and DOC will proactively look for false claims that an organization is a self-certified participant in Privacy Shield via spot checks—including organizations that have let their Privacy Shield certification lapse. Moreover, individuals and DPAs can submit complaints alleging false claims of Privacy Shield participation to both the FTC and DOC.

2) DOC Compliance Reviews – If the DOC receives complaints about a company's Privacy Shield compliance—whether from individuals or from EU DPAs—it will send detailed questionnaires to the company. These questionnaires could be the opening salvo to an administrative or judicial enforcement action.

3) FTC Enforcement of Referrals – The FTC has committed to prioritizing referrals of Privacy Shield noncompliance from EU DPAs and is presently creating a standardized referral process to facilitate its work with DPAs. Upon receiving a referral, the FTC is free to employ any of its standard methods of investigation and, if appropriate, to open an administrative or judicial enforcement proceeding.

Note that Privacy Shield provides that the DOC 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 the DOC's commitment to conduct compliance reviews is supported by an ability to demand all (presumably nonprivileged) Privacy-Shield-related information from an organization at any time.

Depending on the compliance violation at issue, different penalties could result.

1) Removal from Privacy Shield – Organizations that persistently fail to comply with Privacy Shield will be removed from the public list of Privacy Shield organizations and must return or destroy personal data collected under Privacy Shield. These same companies will be "named and shamed" through a DOC list of organizations removed from Privacy Shield and an FTC list of Privacy Shield cases.

2) Agency Enforcement Actions – Even if an organization is not removed from the Privacy Shield organization list, it can find itself subject to a DOC or FTC investigation or enforcement proceeding. Depending on the violations at issue, the FTC can issue a cease-and-desist order or file for a judicial injunction. Violations of an FTC cease-and-desist order can be penalized at up to $16,000 per violation or per day (for ongoing violations).

Importantly, it appears that both the FTC and DOC are taking their enforcement responsibilities seriously. Both have begun hiring additional personnel—in fact, the DOC is *doubling* its enforcement staff—to ensure that they can effectively enforce Privacy Shield compliance.

e. Next Steps

As stated above, it is widely expected that Privacy Shield will be adopted when the Commission issues its final adequacy decision no later than September 2016. Nonetheless, there is a substantial chance that Privacy Shield will be challenged in 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 Commission has publicly stated that it likes Privacy Shield's chances in court. In addition, any appeal to the ECJ will likely take place on a full factual record, and there are many arguments supporting the adequacy of U.S. surveillance-law safeguards that were not briefed for the ECJ in *Schrems*.

With that said, there is significant uncertainty about the future of Privacy Shield. 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 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. In light of this, any company considering using Privacy Shield should do so with the awareness that there is a substantial likelihood Privacy Shield will be challenged in court and a nontrivial risk that it could be overturned.

II. Transfers on the Basis of "Appropriate Safeguards"

When the 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.[18] "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.

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.

"Appropriate safeguard" mechanisms developed under the Directive for permitting transatlantic data transfers include model contractual clauses ("model clauses") and binding

[18] Art. 26(2) Directive & Art. 46(1) GDPR.

corporate rules (BCRs). The GDPR expressly recognizes and permits both of these mechanisms.[19] Additionally, the GDPR creates new transfer mechanisms in the form of approved codes of conduct and certifications.[20]

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) nonnegotiable, which make them advantageous for standard terms as well as for intracorporate arm's-length agreements.

a. Model Clauses Under 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.[21] Moreover, the GDPR expressly provides that model clauses adopted under the Directive will continue in force under the GDPR until amended, replaced, or repealed.[22] Practically speaking, this means that companies that have model clauses in place that predate the GDPR will be able to continue relying on them after the GDPR enters into force in May 2018.

Additionally, 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."[23] 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 that accommodate specific sectorial needs, such as the cloud 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:

[19] Art. 46(2) GDPR.

[20] Article 46(2)(e) GDPR.

[21] Art. 46(2)(c) GDPR; *see also* Art. 28(7) GPDR.

[22] *See* Art. 46(5) GDPR.

[23] *See* Art. 46(2)(d) GDPR.

1) 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.[24] Indeed, it has become common practice throughout the EU to build model clauses 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.[25]

2) 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."[26] 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 contradict mandatory model clauses or 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.

3) Model P2P clauses – To date, the Commission has adopted only controller-to-controller and controller-to-processor model clauses—but no model clauses for processor-to-processor (P2P) transfers. Although model P2P clauses have long been discussed in the EU, and the Article 29 Working Party even went so far as to draft (but not finalize) such clauses, model P2P clauses are presently a rarity in the EU.[27] The GDPR permits both the Commission as well as national DPAs to adopt model P2P clauses.[28]

4) Ad hoc contracts – Finally, the GDPR allows companies to draft ad hoc data transfer agreements and submit them to the competent DPA for approval.[29] These can also be processor-to-processor clauses. It is expected that most DPAs will require ad hoc agreements to largely reflect the provisions of the model clauses (even if that is not a formal requirement).

[24] *See* Commission Decision 2010/87/EC, Annex cl. 10.

[25] Art. 28(6) GDPR.

[26] Recital 109 GDPR.

[27] Spain is one rare country that has produced its own P2P model clauses.

[28] Art. 46(5)-(6), Recital 168 GDPR.

[29] Art. 46(3)(a) GDPR.

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). The GDPR clarifies that transfers on the basis of model clauses do not require any "specific authorization" by a DPA.[30]

b. Next Steps and Practical Expectations

Like adequacy decisions, the GDPR requires the Commission to periodically review the model clauses it has approved.[31] *Schrems*'s 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 once the GDPR enters into force.

Moving forward, we expect DPAs to continue to respect the validity of Commission-approved model clauses as they have to date. Nonetheless, we anticipate many DPAs will begin focusing on whether companies have effectively implemented the clauses. For example, a company that uses model clauses but neglects to disclose them in its privacy notice to consumers would be an easy target for a DPA sanction.[32]

2. Binding Corporate Rules

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

a. BCRs Under the Directive

BCRs developed as an alternative transfer mechanism under the Directive. In 2003 and 2005, the Article 29 Working Party publicly endorsed BCRs as valid bases for international data transfers.[33]

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.

[30] Art. 46(2) GDPR.

[31] *See* Recital 106 GDPR.

[32] *See* Art. 14(1)(f) GDPR (requiring controllers who transfer data on the basis of model clauses to notify individuals that they are using model clauses as the legal basis for the transfers).

[33] *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 downside of BCRs under the Directive's regime was that companies had to obtain BCR approval in a substantial number of European jurisdictions from which they transferred data to the U.S. As an example, one client had to submit its BCRs to the DPAs of 10 different EU member states in order to use those BCRs as a legal basis for data transfers to U.S. affiliate entities. Furthermore, some countries did not simply generally permit companies to transfer data to the U.S. on the basis of BCRs. Instead, they required companies to describe with specificity the individual data streams they intended to transfer on the basis of BCRs and issued permits allowing only those transfers.[34] Thus, any time a company wanted to expand or alter its transatlantic transfers required new notification and permitting procedures.

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.[35] 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 accelerate BCR applications.[36]

The GDPR contains several important changes to existing BCR practices that make them a much more attractive option for businesses:

- BCR-Ps: 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").[37] This was a hotly debated topic during the GDPR's drafting, but BCR-Ps survived and made it into the GDRP's final provisions. It can be anticipated that processors will increasingly rely on BRC-Ps to justify transfers to the U.S. because once BCR-Ps are in place, processors can engage in practically unlimited data transfers to their U.S. co-entities.

- "Model BCRs?" – 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.[38] This could lead to a set of "model BCR"

[34] Examples include Austria, whose DPA required a description of data transfers to be authorized, and Belgium, whose DPA required descriptions of the intended data flows and of all non-EU entities that could receive them. Transfer permits were limited to the data flows and recipients listed on the permit application.

[35] Art. 47 GDPR.

[36] Art. 46(2)(b) GDPR.

[37] *See* Art. 47(3) GDPR.

[38] Art. 47(3) GDPR.

provisions or model BCR approval procedures which, if adopted, would be binding on DPAs and further streamline the BCR approval process.

3. Codes of Conduct and Certifications

The GDPR contains new options for companies to legitimize international transfers in the form of a code of conduct approved by a DPA and/or the Commission[39] and a certification mechanism such as a privacy seal or mark issued by an approved certification body.[40] Controllers or processors in non-EU countries can commit to comply with these mechanisms in order to establish "adequate safeguards" permitting them to receive data transfers from the EU. The GDPR encourages the use of both mechanisms.[41]

a. Codes of Conduct

At present, the Directive permits codes of conduct as a self-regulatory technique to regulate information practices in a specific business sector—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 coregulatory 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 set forth rules that ensure equivalent protection of EU data abroad and 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 an EU controller and a U.S. processor agreeing to implement an approved code of conduct).[42]

The approval of codes of conduct proceeds as follows:

- The association drafting the code of conduct must present it to the DPA having jurisdiction over the international transfers the code seeks to legitimate.[43] If the draft code of conduct relates to processing in only one member state, the DPA may proceed to approve the code.[44]

[39] *See* Arts. 40(2)(i) & 46(2)(e) GDPR.

[40] *See* Art. 46(2)(f) GDPR.

[41] *See* Art. 57(m) & (n) GDPR.

[42] *See* Art. 44(2)(e) GDPR.

[43] Art. 40(5) GDPR.

[44] Art. 40(6) GDPR.

- 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.[45]

- The Board will issue an opinion determining whether the draft code of conduct provides appropriate safeguards for international transfers.[46] 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.[47] The Commission then has the opportunity to determine whether the draft code of conduct has "general validity" throughout the EU. Any such determination would be issued in the form of a Commission Decision.[48]

In keeping with the coregulatory character of codes of conduct, primary compliance monitoring is *not* carried out by DPAs, but by independent "bodies" that have been DPA-accredited.[49] These independent compliance monitoring organizations are empowered to take any "appropriate action" against companies who violate the code of conduct,[50] 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.

b. *Certifications*

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.[51]

The certification process works as follows:

[45] Art. 40(7) GDPR.

[46] *Id*.

[47] Art. 40(8) GDPR.

[48] Art. 40(9) GPDR.

[49] *See* Art. 41(1) GDPR.

[50] *Id*.

[51] *See* Art. 46(2)(f) GDPR.

- 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.[52] 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.[53] 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.

- 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.[54]

- 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.[55]

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.[56] 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 are at present no accredited certification providers, nor are accreditation standards set yet. The Article 29 Working Party has promised to provide guidance on certification at some point in 2016, and this may mark the start of growth of certification infrastructure in the EU.

---

[52] *See* Arts. 43(3), 63 GDPR.

[53] Art. 42(5) GDPR.

[54] *Id*.

[55] Art. 42(6) GDPR.

[56] *See* Arts. 42(7), 43(2)(d) GDPR.

III. Derogations

The Directive established an exclusive list of seven limited exceptions (or "derogations") to the general prohibition on transferring data outside the EU.[57] The GDPR adopts the same list, but adjusts the requirements for claiming derogations in some cases.[58]

Traditionally, reliance on a derogation has not always been favored by DPAs, especially for massive or systematic transfers of personal data.[59] 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 no adequacy decision is present and none of the appropriate safeguards discussed above are available (such as model clauses, BCRs, codes of conduct, or certifications).[60]

As such, companies should not anticipate being able to rely on GDPR derogations for systematic and voluminous data transfers. The GDPR's derogations permitting international transfers are as follows:

1. Consent

Consent was one of the classic legal bases for transfers under the Directive,[61] and the GDPR maintains consent as a transfer basis.[62] Traditionally, consent to an international transfer must be informed, freely given, and unambiguous.[63]

In practice, consent has always been an uncertain basis for transfers, and it will become even more so under the GDPR for several reasons:

- Revocability: Individuals may revoke their consent at any time. In fact, the GDPR requires companies to make revoking consent as easy as giving it[64] and affirmatively inform individuals about their right to withdraw consent.[65]

- Coercion Concerns: Companies have always had trouble showing that consent is freely given. Employee consents are subject to attack before DPAs due to the relationship of

[57] *See* Art. 26(1) Directive.

[58] *See* Art. 49 GDPR.

[59] *See* Art. 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114).

[60] *See* Art. 49(1) GDPR.

[61] *See* Art. 26(1)(a) Directive.

[62] *See* Art. 49(1)(a) GDPR.

[63] *Cf.* Art. 26(1)(a) Directive; Art. 7 GDPR.

[64] *See* Art. 7(3) GDPR.

[65] *See* Art. 14(2)(d) GDPR.

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.[66]

- Informed Consent: 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 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."[67]

These new restrictions may make consent impractical as a transfer basis for some companies. Nonetheless, consent is likely to remain relevant for companies that regularly collect or analyze online behavioral data of EU users, as it may be the only legal basis sufficient to justify extensive profiling-, analytics-, or marketing-related transfers.

2. Other Derogations

The GDPR retains other derogations that are similar to the derogations under the Directive. These include:

1) Contract Performance: Transfers that are necessary for the performance of a contract between the data subject and the controller.[68] The classic example of a data transfer on this basis is a hotel chain sending customer data to the U.S. 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).

2) Third-Party Contracts in the Individual's Interest: Transfers that 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.[69] Examples would include a German travel agency contracting with an American hotel to carry out a German citizen's travel booking, or a French bank retaining an Indian financial institution as a correspondence bank to effect an international wire transfer for an account holder. In both situations, performing the contract requires transferring at least some personal data about the EU subject abroad.

[66] *See* Art. 7(4) GDPR.

[67] Art. 49(1)(a) GDPR.

[68] Art. 49(1)(b) GDPR (similar to Art. 26(1)(b) Directive).

[69] Art. 49(1)(c) GDPR (similar to Art. 26(1)(c) Directive).

3) Public Interest: Transfers necessary for important reasons of public interest.[70] 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."[71]

4) Legal Claims: Transfers necessary for the establishment, exercise, or defense of legal claims.[72]

5) Danger to Life & Limb: Transfers necessary in order to protect the vital interests of the data subject or of other persons when the data subject is physically or legally incapable of giving consent.[73]

6) Transfers from EU Public Registries: Transfers made from a register that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.[74] EU countries maintain a number of public and semipublic registries for different purposes, and this derogation would permit transfers of personal data contained in such registries to the extent the transferor has a right to access such information—for example, transfers of the names of managing employees from a public corporate registry.

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

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."[75]

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 intragroup disclosures.[76] However, the conditions for basing a transfer on the GDPR's new legitimate-interest derogation are *very* restrictive:

1) Only data controllers may rely on this derogation.

[70] Art. 49(1)(d) GDPR (similar in part to Art. 26(1)(d) Directive).

[71] Art. 49(4) GDPR.

[72] Art. 49(1)(e) GDPR (similar to Art. 26(1)(d) Directive).

[73] Art. 49(1)(f) GDPR (similar to Art. 26(1)(e) Directive).

[74] Art. 49(1)(g) GDPR (similar to Art. 26(1)(f) Directive).

[75] Art. 49(1)(h) GDPR.

[76] Recital 47 GDPR.

2) No other data transfer ground can be available, including the other derogations.

3) The transfer(s) at issue cannot be repetitive and can involve only a limited number of data subjects.[77]

4) The controller must assess all the circumstances surrounding the data transfer and based on this assessment adduced suitable safeguards.[78] In selecting privacy safeguards, the processor must 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.[79]

5) The controller must notify the relevant DPA and all affected data subjects that it is relying on this derogation.[80]

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 Noncompliance

Under the Directive, fines for noncompliance 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.

The GDPR dramatically increases the fines available for international transfer violations. 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.[81]

These fines rival the penalties available for antitrust violations and place a premium on setting up transfer infrastructure now so that it will be in place when the GDPR enters into force in May 2018.

V. Conclusion

The GDPR will bring many welcome changes for businesses' data-transfer compliance programs. In general, international transfers will involve far less red tape. Gone are the days of

[77] *Id.*

[78] *Id.*

[79] Recital 113 of the GDPR.

[80] *Id.*

[81] Art. 83(5)(c) GDPR.

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 fines up to € 20 million. 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 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.