Transferring Personal Data Out of the European Union: Which Export Solution Best Fits Your Needs?

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Model contract clauses.*** The most popular option, these require organizations to have a data processing agreement based on the model contract clauses in place with each and every entity with which data is exchanged.
- ***Safe Harbor.*** Disclosures by State Department whistleblower Edward Snowden tainted this self-regulatory framework. Under Safe Harbor, only US organizations may participate — and only through the Federal Trade Commission or US Department of Transportation.
- ***Binding corporate rules.*** Before European reforms in 2012, onerous requirements made this

the least popular option. Now, complying with the proposed regulations, known as the General Data Protection Regulation, means an organization is compliant with most global data protection laws.
- ***How to choose.*** Counsel should weigh factors, including the types of data an organization transfers, the organization's data flows, the locations of corporate entities, cost, effort and ownership within the organization, and more.

In this age of rapid data gathering and exchange, personal data breaches and ever-shifting, culturally-specific perspectives toward privacy, few things are as important to in-house counsel as the appropriate compliance measures, protections and mechanisms for transferring data between the European Union and the United States. In order to understand how we have arrived at the current state of affairs, it is important to review the historical evolution of the relationship between the European Union and the United States when it comes to transferring data.

The main legal mandate in the European Union on data protection is Directive 95/46/EC of the European Parliament and the Council, also known as the Data Protection Directive ("the Directive"). The Directive describes how organizations should best handle, transfer and process personal information. Further, an organization may only transfer data outside of the European Economic Area (EEA) (which, in addition to the European Union member states includes Iceland, Liechtenstein and Norway) if, based on European Union standards, it provides an adequate level of protection for the data in the recipient non-EEA territory. The rationale behind the Directive was that although some member states had already adopted national data protection laws, in order to move goods, services and data throughout the European Union, each member state should be able to rely on a harmonized high level of data protection. Though the European Union had a strong foundation with respect to an individual's innate right to privacy, the Directive gave these principles some real teeth.

Remember, 1995 was a time before you could purchase your plane ticket, groceries, clothing and practically anything else online, before you entered your health data into an online database, before you watched TV on your computer and definitely before cookies were something other than an afternoon treat.

Before delving into the various mechanisms available to transfer data from the European Union to the United States, for purposes of context, it is important to quickly review some applicable legal definitions:

- *Personal data* is any information relating to an identified or identifiable natural person (also referred to as the data subject). For in-house counsel normally familiar with the more US-centric concept of identifying an individual, it is critical to understand that, under the Directive, an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. As a practical example, in the United States, an Internet protocol (IP) address is not generally considered personal data; whereas under the Directive, because an IP address may be linked with other identifying personal information, this makes a data subject identifiable and would be considered personal data. In the European Union, the presence of personally identifiable information (PII) triggers the application of data protection laws. The EU approach comprises all information that is identifiable to a person as PII, a broad and all-encompassing approach. Comparatively, the

US approach tends to be commercially driven: it is narrow, specific and divergent between states and the federal government. Scholars and practitioners alike generally consider the differences between the two approaches to be irreconcilable.

- *Processing of personal data* is any operation or set of operations that is performed on personal data, whether by automatic means or not, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination blocking, erasure or destruction. In practical terms, this is anything that an organization does with data. The key thing to note here is how broad this definition is — if you are not sure whether your organization is processing data, it probably is.
- *Data controller* is the natural or legal person, public authority, agency or any other body that alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or community law. Again, from a practical standpoint, this is the organization that makes decisions about the data. Typically, in a supply context, the service provider will be a data processor. Essentially, if your organization is deciding what kind of personal data it will collect, how it will use it and who will have access to it — you are the controller. As the controller carries with it the most serious legal responsibilities, it is very important to understand which side of the data line your organization is toeing. For example, most organizations are the controllers for their employee data and they outsource processing, such as payroll and travel, to vendors.
- *Data processor* is the natural or Callout legal person, public authority, agency or any other body that processes personal data on behalf of a controller. It is helpful to think of the processor as an organization that does not actually have control of the data, but rather performs specific tasks assigned to it by the organization which is the data controller (e.g., a payroll company). When it comes to performing this analysis, please note that with the same large group of data, an organization may be a controller with respect to one set of data and a processor with respect to another. In a service provision context, the service provider will normally be a data processor and its customer the data controller.

Please keep in mind that where a data subject has provided unambiguous consent or another specific derogation recognized under the Directive, the organization may not require a data transfer mechanism. However, the Article 29 Working Party (the advisory arm under the Directive) recommends that the "… derogations should be interpreted restrictively and preferably be applied to cases in which it would be genuinely inappropriate, or even impossible, for the transfer to take place…" under a recognized cross border data transfer mechanism. With these basic concepts in mind, what options do organizations currently have in order to transfer personal data out of the European Union? In the next section, the three currently accepted mechanisms for cross border data transfer are discussed: model contract clauses, the EU/US Safe Harbor, and Binding Corporate Rules (BCRs).

Model contract clauses

Both the Council of Europe and the European Parliament gave the European Commission the ability to determine whether certain standard contractual clauses (frequently referred to as the model contract clauses) will provide for adequate safeguards of personal information for the purposes of Article 26(2) of the Directive. With help from the Article 29 Working Party, the European Commission developed, and subsequently revised, standard model contract clauses to govern both the data controller to data controller and data controller to data processor relationships. While the model

contract clauses are still the most popular option that organizations use to transfer data out of the European Union, the inherent problem with the clauses for large organizations is the need to have a data processing agreement based on the model contract clauses in place with each and every entity with whom data is exchanged — which can turn into quite an administrative burden to manage appropriately.

Safe Harbor

Specifically to facilitate data exchange between the European Union and United States, between the years 1998–2000, the United States Department of Commerce and the European Commission negotiated a framework (known as Safe Harbor) that bridges the differences between the United States and European Union approaches, processes and laws with respect to data protection. Likewise, a Safe Harbor is also available between Switzerland and the United States.

When the framework was finalized in 2000, companies were able to self-certify that they were in compliance with the Safe Harbor requirements. Between the years 2000 and 2013, over four thousand organizations adopted Safe Harbor; however, in the same time frame, the European Union became quite distrustful of the mechanism as it allowed for self-reporting. The Federal Trade Commission (FTC), the United States regulatory body in charge of oversight, was not engaging in the kind of enforcement the European Union wanted to see. Though there was already a somewhat skeptical attitude toward Safe Harbor, the revelations of US government activity provided by Edward Snowden created significant pressure to reform the existing framework. Some in-house counsel of US companies found themselves in situations where European partners refused to continue to exchange data under Safe Harbor.

Importantly, not all organizations in the United States are eligible to participate in Safe Harbor. In general, an organization is subject to enforcement under federal or state laws for unfair or deceptive trade practices. Specifically, the FTC and the US Department of Transportation (for air carriers and ticket agents) have both committed to the European Commission that they will enforce violations of the Safe Harbor against organizations that have signed up for this self-regulation regime. Thus, only organizations governed by these two agencies are eligible to participate in the Safe Harbor program.

Binding corporate rules

Binding corporate rules (BCRs) have received quite a bit of press attention lately, but have existed since 2003. At the time, the process to implement BCRs was quite onerous and lengthy. Each member state was required to individually approve the application. This discouraged organizations from pursuing BCRs, with only 19 organizations globally completing the process in 2012.

However, in 2012, the European Commission proposed reforming the existing data protection laws in order to address some of the obvious problems that had arisen since 1995 and, perhaps more importantly, unify the existing data protection laws within the various European Union member states into a single law. Though the proposed regulations (known as the General Data Protection Regulation or GDPR) would make for an article in its own right, there has been an overwhelming consensus among leaders of the European privacy law reform movement that BCRs provide a significantly more robust mechanism to transfer data out of the European Union within a defined corporate group. BCRs eliminate the issues with both Safe Harbor and the model contracts, while still providing for the kind of accountability the European Union requires.

BCRs are a set of rigorous rules, codes or practices based on European data protection standards, backed by training and audit programs, and approved by the national data protection authorities (DPAs) through a process known as mutual recognition. Mutual recognition has been adopted by 21 of the 28 members states and significantly reduces the time and effort taken to complete a BCR application. BCRs are available to both data controllers and data processors and permit the flow of data within the defined corporate group, no matter where the entities are located. Their key strength is that they encourage the implementation and maintenance of a full-fledged accountable privacy program within the business, rather than a quick fix legal solution like model clauses or Safe Harbor. Though, as with all such mechanisms, it is not a panacea and BCRs require significant time and financial commitment. If your company transfers volumes of data out of the European Union or prides itself on being an industry leader in terms of data security, BCRs might be just the tool you need. As an added bonus, since European data protection and privacy laws are quite strict, complying with the BCRs likely means your organization will comply with most global data protection laws as they stand today.

In this next section, we will provide a short-form comparison of the three data transfer mechanisms discussed previously.

What are the benefits to each solution?

Model Contract Clauses

- Simple to execute
- Straightforward check-the-box solution
- Expressly recognized by all European Economic Area DPAs
- Applicable to data exports globally
- Both controllers and data processors can use these

Binding Corporate Rules

- No limits geographically on data transfers within a group of companies
- Recognized as the highest standard in data exports
- Considered future-proofed because this mechanism is expressly mentioned in the recent EU data reform laws
- May be used as a comprehensive data governance framework
- Both controllers and data processors can use these

EU/US Safe Harbor

- Self-certification process
- In use by over 4,000 US companies
- Enforced by a US agency, which is generally desirable to organizations in the United States
- Accommodates onward transfers to third party agents, who are not necessarily part of the same corporate group, outside the United States only after data is received in the United States (you should not take for granted that you can export data to subsidiaries and affiliates located outside the United States)
- EU entities can easily verify if US processor is part of the Safe Harbor program
- Due to criticisms, now has enhanced privacy enforcement cooperation (memo of understanding signed with United Kingdom). The FTC has increased enforcement activities

How easily can a global company implement the respective mechanisms?

Model Contract Clauses

- Tried and trusted solution
- Very quick and easy to execute
- No need for regulatory approvals
- Enables transfers globally (not just US)
- Seldom (never?) enforced

Binding Corporate Rules

- Can be tailored to internal culture and processes
- PR uplift — BCRs are akin to a data protection trust mark
- Great relationship building with EU DPAs
- Institutes training, audit and compliance structure requirements
- Recognized throughout the EU
- Often used as guidance by non-EU countries for their requirements

What is sensitive personal data?

The European Union defines sensitive personal data as “data revealing racial origin, political opinions or religious or philosophical beliefs, trade-union membership and data concerning health or sex life.” Is this definition consistent globally? We reviewed the definitions of sensitive personal data in various countries.

In the United States, there is no national definition for sensitive data, although some forms of data require more protection than others, such as medical, student or financial data. However, in the global realm, we start seeing some variation. In general, the definition above in Europe holds true for most nations that define sensitive information. Some nations, like Canada, Columbia, Egypt, Israel and Mexico, do not necessarily call out a specific definition for sensitive personal data, but rather expects such data to be identified and protected to a higher degree. It’s a judgment call.

Fourteen nations do specify that information related to criminal records, investigations and proceedings are considered sensitive personal data, and some go so far as to also say administrative proceedings are equally sensitive. This is quite different than in the United States where arrest records are public, although perhaps not so easy to find everywhere — but certainly convictions and proceedings are not only public, but often televised.

Last, there are some interesting additions to the definition of certain sensitive data, usually in one country. Hungary includes “abnormal addictions.” Australia adds biometrics, as do the Czech Republic and Azerbaijan. Azerbaijan also includes domestic violence, marriage or family matters, child adoption, social welfare and taxes. The Philippines include age and education. Israel, however, does specify that one’s personality is sensitive personal data.

EU/US Safe Harbor

- Straightforward process, easy to adopt
- Good flexibility for subcontracting data processing
- Avoids the needs for exponential model contracts
- The simplest solution for a US data importer

What are the main challenges of each mechanism?

Model Contract Clauses

- Model Contract Clauses require a contract for each export of data — could mean hundreds of contracts
- Not commercially friendly
- Strict restrictions on subcontracting, e.g. requiring full flow down of contractual terms to subcontractors
- Some joint and several liability (e.g., data importer can be held liable for breaches of data exporter, under some versions of the model clauses
- Criticized for not providing a practical solution for compliance, merely for complying with need to use something
- Is merely contractual, does not provide a usable data protection framework
- No negotiation on the language in the clauses is permitted (although some companies do. Any changes make them then non-standard and outside the approved process)

Binding Corporate Rules

- Complex, thorough and intense process
- Time commitment as authorization may take a total of 18–24 months
- Resource commitment — organization must comply with the policy requirements of BCRs
- Requires auditing — permits internal or external, but must describe in application
- Valid only for inter-organization data transfers within the same corporate group

EU/US Safe Harbor

- Currently going through process of reform
- Uncertain future under EU GDPR
- Strictly speaking, is a controller-only solution
- Not available to organizations not regulated by the FTC, such as financial services clients

Other than the challenges above, what are the real-life considerations with each mechanism?

Model Contract Clauses

- Not so well-loved by privacy professionals, because they are an administrative burden and do not appear to deliver actual compliance
- EU regulators love the clauses, despite their impractical nature
- Very unpopular among cloud suppliers due to subcontracting restrictions and need for exponential contracts

Binding Corporate Rules

- Considered the “gold standard” in the EU — by regulators and customers alike
- Historically have had a bad reputation for a complex and expensive approval process, which has become much simpler
- Not a common solution, so EU customers may still ask for EU/US Safe Harbor or Model Contract Clauses

EU/US Safe Harbor

- EU Parliament and EU Commission consider it the “Not So Safe Harbor”
- Concerns that self-certification commitments are merely checkmarks without accountability
- Criticized by European regulators for limited enforcement to date, although it is being addressed
- Not acceptable to all European customers, who may require additional data protection assurances — means that deals can collapse where Safe Harbor is the only solution offered
- Privacy groups and national data protection authorities often view Safe Harbor with skepticism

How does each mechanism work with sensitive personal data?

Sensitive personal data is defined in the Directive as data revealing racial origin, political opinions or religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.

Model Contract Clauses

- Can be used to transfer sensitive personal data
- Data exporter must inform individuals their data being sent to a processor in an “unsafe” country
- Onward transfers to third parties generally require consent

Binding Corporate Rules

- Can be used to transfer sensitive personal data
- No express requirements for sensitive personal data, other than it must be processed in accordance with EU standards

EU/US Safe Harbor

- Can be used to transfer sensitive information
- Explicit opt-in required for transfers to a third party or repurposing
- Not clear what is “sensitive” for Safe Harbor purposes — uses the term “sensitive information” rather than EU term of “sensitive personal data”

Do the mechanisms work both directions for data flows (EU to the rest of the world “RoW” and vice-versa)?

Model Contract Clauses

- Permits data transfers from EU to anywhere in the world
- Envisions only one way transfer flows — from EU to RoW

Binding Corporate Rules

- A global solution — Binding Corporate Rules meet and exceed most countries' data protection requirements
- Explicitly compatible with Asia-Pacific Cross-Border Privacy Rules

Cross border privacy rules in the Asia Pacific region

In November 2011, the Asia Pacific Economic Cooperation (APEC) leaders issued a directive to initiate and develop a system of cross border privacy rules (CBPRs) derived from the 2005 APEC Privacy Framework. The APEC Privacy Framework was based on the 1980 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data issued by the Organisation for Economic Co-operation and Development. Essentially, the APEC member economies have recognized the importance of data protection along with the impact of technology on the use and sharing of data, and that they, like to European Union, need rules in place to govern the transborder flow of personal data. The CBPRs requires organizations to develop privacy practices consistent with the APEC privacy framework and consists of four aspects: self-assessment, compliance review, recognition/acceptance and dispute resolution and enforcement. An accountability agent must then certify that the organization is compliant with the CBPRs and resolve any disputes.

The participating member economies so far consist of Japan, the United States and Mexico. Canada has announced its intention to join. Each country must provide an accountability agent. Currently, the only accountability agent that has been approved is TRUSTe. Ten companies have successfully completed the approval process (all from the United States). Japan and Mexico have yet to identify theirs. To further the goals of the CBPRs, an APEC/European Union joint working group published the Referential, a detailed comparison between the APEC CBPRs and the European Union binding corporate rules. This Referential does not create any sort of mutual recognition, but merely makes it easier to quickly understand the similarities and differences between the two cross border data transfer regimes.

EU/US Safe Harbor

- Allows data transfers from the EU and there is another Safe Harbor for Switzerland to the United States
- Limited global interoperability
- An inbound data transfer solution only
- Onward transfers intra-company are technically only possible once data is received in the United States and onward transferred in compliance with safe harbor standards

How much do the mechanisms cost in money and effort?

Model Contract Clauses

- Front End $ (proscribed template)
- Back end $$ (need personnel to manage, monitor and enforce)
- Standard form contract, populate the annex (describing data, processing, etc.), sign and done

- Eliminates negotiation on language

Binding Corporate Rules

- Front End $$$ (preparation and filing, may include bringing activities and processes into compliance with BCR requirements)
- Back End $ (assuming activities/processes are made compliant in front end work)
- Typical budget about USD $220,000, depending on efficiency and “lead authority”
- Timeline around 18–24 months start to finish

EU/US Safe Harbor

- Front End $–$$$ (depends on approach: get certified or get compliant)
- Back End $–$$$ (same as above; checking the box or being compliant)
- Submitting a Safe Harbor certification is minimal cost — little paperwork involved
- Real expense is in bringing practices in line with Safe Harbor commitments

Do the respective mechanisms work best depending on the size of the business?

Model Contract Clauses

- Small business can get maximum benefit from this mechanism
- Large businesses need many contracts to meet their data transfer needs
- Impossible to use in a cloud environment

Binding Corporate Rules

- Maximum impact for high growth or blue chip businesses (time and resource needs)
- Becoming more attractive to smaller businesses due to simpler process
- Truly impactful for global companies

EU/US Safe Harbor

- Equally viable for large and small businesses
- Commonly used by US start-ups as it is easy to implement, cookie cutter solution, known process
- Administratively much simpler than Model Contract Clauses

What does the enforcement regime look like for each mechanism?

Model Contract Clauses

- Enforcement by EU DPAs
- Individuals have third-party rights
- Some Model Contract Clauses include joint and several liability provisions
- Processors can be held liable for breaches by their controller, albeit unlikely
- Seldom enforced in practice

Binding Corporate Rules

- Enforcement by EU DPAs
- Individuals have third-party rights
- Processors can be held liable for breaches by their controller, albeit unlikely
- The internal complaints procedure in BCRs is intended to resolve most complaints
- No known DPA enforcement to date

EU/US Safe Harbor

- Enforcement by FTC
- >20 cases of enforcement to date — and most of it in 2014!
- Enforcement by EU DPAs for HR data
- Need for third-party dispute resolution provider

The road to BCRs

BY K ROYAL

Now, this is the story all about how my life got flipped, turned upside down… I was new to Align Technology Inc. when we started looking outside the model contract clause avenue to cross border data transfers out of Europe. We had recognized how burdensome the model contracts are to manage. Over 3,000 US companies were signed up to the EU/US safe harbor; only 19 companies globally had BCRs.

April, 2012	Hired an outside law firm and a large consulting company to evaluate the pros/cons of both mechanisms. Involved internal working group. Met with executive stakeholders. Determined lead DPA (Dutch). Ensured DPA registrations were updated and complete.
July, 2012	Decided to pursue BCRs.
Sept., 2012	Met with Dutch DPA. There was no processor BCR application. We worked with law firm to create a process; DPA supported plan.
Jan., 2013	EU issued processor BCR application. Reformatted our work. April, 2013 ONE YEAR — filed dual application for processor/controller BCRs. During the past year, assessed policies and processes to comply. Developed roadmap of changes and improvements. Continued this work once application was filed.
Aug., 2013	Received comments from lead DPA.
Oct., 2013	Filed response.
Nov., 2013	Follow-up comment from lead DPA. Response filed.
Dec., 2013	Lead DPA circulated applications to reviewing DPAs (UK and Spain) under the mutual recognition.

Feb., 2014	Spanish DPA indicated approval.
March, 2014	UK portion completed. Lead DPA circulated to seven DPAs which are not part of mutual recognition.
May 2, 2014	BCRs successfully closed.
June, 2014	DPA registrations updated with BCRs.

What went well working with FieldFisher was the best part of the process. We originally reformatted all of their draft policies into the company format — and had to reverse them. FieldFisher was wonderful in working with our notions of commercial viability. We, in the United States, like to ascribe meaning to certain phrases that are not so contentious in the European Union.

Socializing policies and gathering feedback may seem valuable to us from a business perspective, but realistically, there is not much that can be changed in required BCR policies.

Conclusion and recommendations

Determining the appropriate cross-border transfer mechanism is not a decision to be taken lightly. In-house counsel must consider and weigh multiple factors including the types of data your organization transfers, your organization's data flows, the locations of your corporate entities, cost, effort and ownership within your organization and much more.

On a practical level, consider whether you desire to maintain a bifurcated approach (handling US personal data differently than you do EU PII) or whether you desire one global approach using the strictest requirements as your baseline. In the bifurcated approach, you could also choose to place a server in the European Union for all EU data that can only be accessed by people in the European Union. If you can successfully manage a data segregated approach, you may not need a data transfer mechanism. However, it is rare that total data segregation truly works for a global company. This might differ based on your company, product and services offerings and type of data being transferred.

Before making any decision, we recommend engaging in a basic, yet often overlooked, useful activity: mapping your data. If the person providing the data is in the European Union, the EU rules apply. If the data enters the European Union (other than the data merely being in transit where it is not accessed or manipulated), the EU rules apply. Know what elements of PII you collect, where you store it, who sees it and how it is used and protected. You should only collect the PII you absolutely need and delete it when its purpose has been served.

Last, we recommend reviewing contracts and business relationships. Once you've determined if and how you want to transfer data across borders in view of the available data transfer mechanisms and mapped your data, you need to operationalize your approach. A large part of this includes examining your relationships and contractual obligations. You may need to renegotiate agreements both from the controller and processor sides. We hope with the information presented in this article, you can better determine what solution best fits your needs as there is no one-size-fits-all model. As your organization grows and evolves, so may your data transfer needs. The one consideration that stands out is that international data protection requirements are getting stronger every day (and there is a rumor that the GDPRs may carry with them a hefty fine for non-compliance — up to five percent of

global turnover).

Further Reading

Directive 95/46/EC of the European Parliament and of the Council, OJ 1995 L 281.

Agreement on the European Economic Area, OJ 1994 L 1.

Directive 95/46/EC of the European Parliament and of the Council, Article 2(a) OJ 1995 L 281.

Directive 95/46/EC of the European Parliament and of the Council, Article 2(b) OJ 1995 L 281.

Directive 95/46/EC of the European Parliament and of the Council, Article 2(d) OJ 1995 L 281.

Directive 95/46/EC of the European Parliament and of the Council, Article 2(e) OJ 1995 L 281.

Katia Bloom

Commercial Lawyer and Associate General Counsel

ForgeRock

Katia Bloom is a fast-paced and strategic commercial lawyer. Currently, she is the associate general counsel at ForgeRock. Previously, she headed up legal for Avira, Inc., was a founding partner at E Squared Law Group, advising many start-up clients and was in-house counsel at Anesiva. She is actively involved in the Association of Corporate Counsel and a number of organizations promoting women in the legal profession.

K Royal

Global Chief Privacy Officer

Crawford & Company

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.