Bloomberg BNA

Privacy and Security Law Report®

Cross-Border Information Sharing for Effective Services

BY MIRIAM WUGMEISTER AND KARIN RETZER

Services today are driven by information. Having access to and using the right information at the right time are essential to the efficient provision of services. However, timely access to information is complicated by myriad privacy laws.

Navigating privacy laws is especially challenging for U.S.-headquartered companies with affiliates in the European Economic Area (EEA)[1] who wish to share personal information with U.S.-based service providers. Data flows are complex, and companies will need to ensure compliance with cross-border restrictions. All member countries of the EEA impose restrictions on the sharing of personal information outside the EEA. Organizations sharing personal information collected in the EEA with service providers based outside the EEA (often in the United States) must find ways to comply with these laws while at the same time effectively utilizing service providers around the globe.

Companies must first consider whether these cross-border restrictions are relevant to their business. Generally speaking, in order for the EEA laws and regulations to apply, an organization must be established in an EEA country. That means the organization must be incorporated in an EEA country, have a stable and permanent presence there, or use equipment located in an EEA country to process personal information. The obligations that constrain how information can be shared across borders turn on how personal information flows from entities in the EEA to service providers. While this is counterintuitive, how the data actually flow matters in determining how the cross-border rules apply and what mechanisms are necessary to meet those obligations.

In many instances, multinational companies share personal information first with an affiliate in the United States and then transfer the personal information to a service provider. For example, a French company or employees of the French company may send personal information relating to its employees first to its U.S.-based parent company, and then the U.S. parent company will provide the information to a service provider. In other instances, information from an EEA company is shared directly with a U.S.-based service provider, such as personal information provided by employees of a French affiliate via phone or through a website hosted or run by a service provider in the United States.

We will examine each of these types of data flows and discuss what mechanism is required to legitimize each transfer.

Indirect Transfers to Service Providers

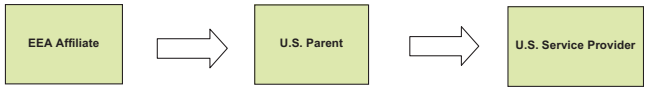
Personal information often flows indirectly between the location where the information is collected and a service provider who will ultimately handle the personal information. One common occurrence is a transfer of information from a company in the EEA to its U.S.-based parent company that then shares the personal information with a U.S.-based service provider. For example, a multinational company that establishes a centralized human resources ("HR") system will host it at its U.S. headquarters. The U.S. headquarters then shares certain HR information with a service provider in the United States in order to provide benefit services to the company's global workforce.

The restrictions imposed on information sharing with a service provider in the United States depend in part on the transfer mechanism chosen by the EEA affiliate and the U.S. parent to transfer the information between

[1] The EEA includes all EU member states, plus Iceland, Liechtenstein, and Norway.

Miriam Wugmeister, a partner at Morrison & Foerster LLP's New York City office, is a member of the firm's Global Privacy and Data Security practice. She is also a member of the advisory board for the Privacy & Security Law Report. Karin Retzer, also a member of Morrison & Foerster's Global Privacy and Data Security practice, is a partner in the firm's Brussels office.

 ISSN 1538-3423



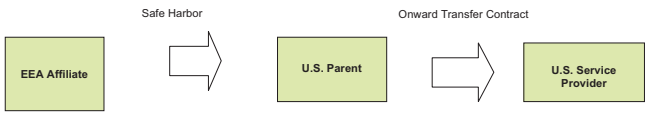
the EEA affiliates and the U.S. parent company. The EU Data Protection Directive (95/46/EC) (the ''Directive'') restricts any transfers of personal information to countries outside the EEA, unless the recipient country has been found to ensure an ''adequate'' level of protection.[2] The question of whether adequate protection exists is generally decided by the European Commission (EC) or national information protection authorities. Very few adequacy decisions have been made, however, since the EU data protection obligations were enacted in 1995. So far, only the laws of Andorra, Argentina, Canada, the Channel Islands (Guernsey and Jersey), the Faeroe Islands, the Isle of Man, Israel, New Zealand, Switzerland, and Uruguay have been recognized as adequate.

There are essentially five mechanisms for transferring personal information from an EEA affiliate to a parent company in the U.S.:

- the U.S. parent has been certified by the U.S.-EU Safe Harbor Framework;
- the individual has given his or her unambiguous consent;
- the transfer is necessary for the performance of the contract with, or concluded in the interests of, the individual;
- the EEA affiliates and the U.S. parent have entered into an appropriate contract which, if individually negotiated, may require approval of the EU member state authorities (''ad hoc contracts''), or which incorporates certain Standard Contractual Clauses that have been approved by the EC; or
- the customer and the affiliates receive the information subject to an approved set of Binding Corporate Rules (BCRs), which also require the approval of the EU member state authorities.

We will discuss each in turn and look at the effects that the chosen adequacy mechanism has on the transfer of personal information to a service provider.

Safe Harbor



The Safe Harbor Framework was developed by the U.S. Department of Commerce in consultation with the EC,[3] and consists of a set of seven ''Safe Harbor Privacy Principles'' and 15 ''Frequently Asked Questions'' (FAQs), as well as the EC's adequacy decisions.[4] To take advantage of the Safe Harbor, a U.S. company must voluntarily elect to comply with the Safe Harbor Principles and the FAQs, identify in its privacy policies that it adheres to Safe Harbor, and certify its compliance with the U.S. Department of Commerce.

Although there has been criticism of the Safe Harbor from varied sources, recent pronouncements by the EC and the U.S. Department of Commerce indicate that the Safe Harbor remains a legitimate and highly valued cross-border mechanism for the sharing of information between the EEA and the United States.

Where a U.S. parent company has elected to join the Safe Harbor, personal information from its EEA affiliates can be transferred to the U.S. parent company.[5] The U.S. parent company then must comply with the Safe Harbor Principles regarding ''onward transfer'' when it elects to share the information with a service provider.

The onward transfer principle requires that a written onward transfer agreement be put in place between the U.S. Safe Harbor-certified entity and the service provider. Onward transfer agreements are generally short and simple agreements that seek to downstream the relevant Safe Harbor obligations to a service provider. Onward transfer agreements require that the service provider use and protect personal information in compliance with the Safe Harbor Principles, but does not impose additional obligations and liabilities found under the Standard Contractual Clauses.[6] Thus, Safe Har-

[2] Directive 95/46/EC, of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281/31), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF. The Directive applies to all EEA member states.

[3] In 2009, the U.S. Department of Commerce established a similar ''Safe Harbor'' framework in consultation with the Federal Data Protection and Information Commission of Switzerland to bridge the different privacy approaches between the two countries and provide a streamlined means for U.S. organizations to comply with Swiss data protection laws. U.S.-Swiss Safe Framework, *available at* http://export.gov/safeharbor/swiss/index.asp.

[4] U.S. Dep't of Commerce, *Safe Harbor Privacy Principles* (July 21, 2000), *available at* http://export.gov/safeharbor/eu/eg_main_018475.asp; U.S. Dep't of Commerce, *Frequently Asked Questions (FAQs)*, *available at* http://export.gov/safeharbor/eu/eg_main_018493.asp; European Commission, *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last updated July 16, 2013).

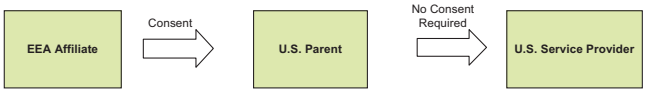
[5] Not all U.S. organizations may certify to the Safe Harbor. For a U.S. organization to be eligible for the Safe Harbor, it must be subject to the jurisdiction of a government body such as the Federal Trade Commission (FTC) which is empowered to investigate complaints and to obtain relief against unfair and deceptive practices. Article 1.2 of 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce (L 215/7), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF. At present, only the FTC (under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45) and the Department of Transportation (under 49 U.S.C. § 41712, which covers air carriers) satisfy this requirement. As a result, only organizations subject to the jurisdiction of either of those two agencies are eligible to join the Safe Harbor. Thus, financial institutions, for example, are not eligible to join the Safe Harbor.

[6] The Safe Harbor principle on ''onward transfer'' provides: ''Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or an-

   ISSN 1538-3423

bor onward transfer agreements are much more straightforward than the Standard Contractual Clauses adopted by the EC and far easier to negotiate and execute than the individual entities' Standard Contractual Clauses.

Consent



Obtaining individuals' unambiguous consent may authorize the transfer of personal information under most EU member state laws. There has been a great deal of attention paid to the statements by some data protection authorities regarding the use of consent. Debate continues in the EEA as to whether it is appropriate to rely on consent obtained from employees as a legal basis for transfer. The concern is that employees cannot freely consent to such transfers due to the perceived imbalance of power between employers and employees. In order for consent to be valid, individuals must be permitted to withdraw their consent without suffering adverse consequences.

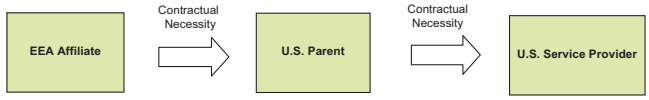
Despite the fact that consent is said to be ''invalid'' in the employment context, most EU member states require an opt-in consent for the sharing of ''sensitive'' information (i.e., health information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information specifying the sex life of the individual) with a third party, even with an affiliate. Thus, although consent may in theory not be valid, it is still required in many instances.

What this means in practice is not always clear. In the data protection context, consent must be ''informed,'' which means it is based on a notice explaining in detail what information is collected, how the information will be used and shared, the potential recipients, and how individuals can exercise their mandatory rights of access and correction in relation to their personal information. Thus, in order for the consent to be valid, the individual must be provided with these details. A high-level notice in which an employee simply agrees to participate in a benefit plan or a stock option plan would not be enough. Conversely, if a notice were sufficiently detailed about the collection, use, and disclosure of personal information, and the individual truly had a choice as to whether or not to share his or her personal information, a consent would be valid in most countries.

If employees of an EEA company are provided with a clear and detailed choice concerning whether or not their information will be shared with a U.S. parent company and they consent to that sharing (for example, to participate in a stock option plan), there is generally no need to obtain further consent in order for the U.S. parent company to share the information with a service provider. In most EEA countries, individuals must be informed that personal information will be shared with a service provider, but consent is not required for that sharing. In some EEA countries, the EEA company may be required to disclose the specific name of the service provider, not just the type of service provider or country. These requirements are usually addressed in the notice and consent for the initial sharing with the U.S. parent company, and there is no additional compliance step to then share the information with the service provider if the initial consent was sufficiently broad and valid, and individuals are aware that information will be shared with service providers in the United States.

Thus, depending on the circumstances and the country, consent may be a valid alternative for sharing personal information with a U.S. parent company and then with service providers.

Contractual Necessity



Data protection authorities in the EEA also allow transfers of personal information where the information is necessary for the performance of a contract with the individual, or for the performance of a contract between the transferring entity and a third party which benefits the individual. In some instances, the U.S. entity enters into a direct contractual relationship with the individual. Thus, for example, if a company in the United States wishes to provide stock options to its employees in the EEA, certain personal information must be transferred to the U.S. The employer in the EEA could rely on contractual necessity to transfer the needed information. This would cover both transfers to the U.S. parent company as well as to the service provider. Similarly, sharing information with a service provider to provide employee benefits would be covered by the contractual necessity exception.

Although this may seem to be the most straightforward basis on which to rely when transferring personal information, the information that can be transferred under this approach is quite limited and such a transfer must be truly ''necessary'' to meet the contractual obligations. Several EEA member states view information that is ''necessary to complete a contract'' narrowly, i.e., limited to that which is ''indispensable.'' For example, German authorities argue that where a German employer transfers specific employee data to U.S.-based insurance providers and the insurance contract provides for third-party beneficiary rights for the employee, such transfer is permitted because of contractual necessity.[7] However, cost-cutting or centralizing data to create greater efficiency would not generally be recognized as sufficient grounds to justify or necessitate the transfer based on contractual necessity.[8]

Thus, for limited sets of data that are truly needed in order to fulfill a contractual agreement with employees,

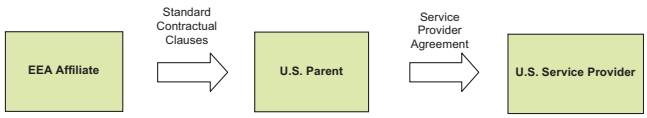
other adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles.'' The *Safe Harbor Privacy Principles*, including the principle on ''onward transfer,'' are available at http://export.gov/safeharbor/eu/eg_main_018475.asp. *Safe Harbor Privacy Principles*, *supra* note 3. This is not the same as the Standard Contractual Clauses.

[7] *See Arbeitsbericht der ad-hoc-Arbeitsgruppe ''Konzerninterner Datentransfer,'' available at* https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Personalwesen/Inhalt/5_Beschaeftigtendatenschutz_Konzern/arbeitspapier_ad_hoc_idv.pdf.

[8] *Id.*

contractual necessity may be a valuable and viable alternative.

Transfer Contracts



Transfers are also allowed where an EEA company enters into a data transfer contract with a U.S. parent company. Contracts tailored to the parties' needs (ad hoc contracts) must generally be pre-approved by all data protection authorities in all the countries through which information is transferred. Thus, ad hoc contracts are expensive and difficult to implement and are rarely used. Alternatively, the EEA company and the U.S. parent company may enter into the Standard Contractual Clauses adopted by the EC. These clauses were intended to streamline the process, and thus no approval of the actual substantive provisions of the clauses is required. The reason that there are no approval requirements for the substantive provisions is that the clauses cannot be altered. In order for them to be valid, nothing can be modified or changed in the substantive provisions. There are a few different versions of the clauses, but for transfers from an EEA affiliate to a U.S. parent company, the ''Controller to Controller'' set of clauses is generally set forth in the relevant contract.[9]

Contracts can be very difficult to administer. Information flows do not always follow along neat or well-established paths and may move along a multitude of paths and channels through email exchanges, information bases, and intranets. Global organizations have complex structures that can change frequently. Unless regularly revised, contracts will not reflect the changes in usage of information in organizations as required under the EC contract law regime.

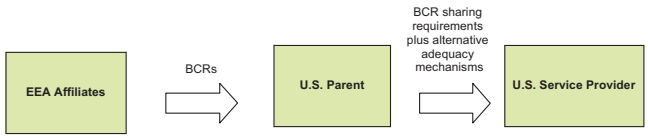
Under the Controller to Controller clauses, the U.S. parent company may share information with a service provider if ''procedures'' are in place to ensure that the service provider will ''respect and maintain the confidentiality and security of the personal data.''[10] In other words, as long as the U.S. parent company has an agreement with the service provider that requires the service provider to maintain appropriate data security standards and confidentiality protections, and limits the service provider to using the personal information only as instructed by the U.S. parent company, the obligations of the U.S. parent company are satisfied. This agreement does not need to be in a set form and can be different from the Standard Contractual Clauses; it can also be kept in a flexible state.

Binding Corporate Rules

Some organizations elect to adopt a set of BCRs to enable transfers from EEA affiliates to other members of the corporate family. BCRs allow companies to establish safeguards without the administrative, legal, and organizational complexities of implementing standard contracts. A set of BCRs can be tailored to the specific needs of each organization but must be limited to share information only within the corporate family.

Adopting a set of BCRs does not alter the need for an adequacy mechanism for sharing information with service providers. As a result, any restrictions imposed on sharing personal information with service providers is often addressed in the BCRs, but one of the other adequacy mechanisms, such as Standard Contractual Clauses, Safe Harbor certification, or contractual necessity, will be required.

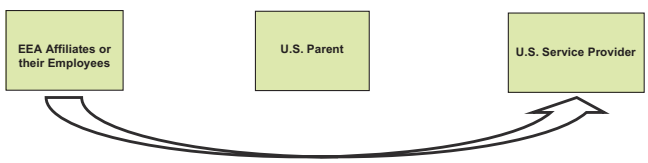
To date, however, very few companies have adopted BCRs, given the significant cost and time involved in establishing such a framework and obtaining the necessary approvals from the data protection authorities. For most BCRs, the approval process takes a substantial amount of time (often years) and requires much internal realignment of policies and procedures.



Direct Transfers to Service Providers

In some cases companies in the EEA may share information directly with a U.S.-based service provider. These data flows often occur when individual employees interact with a service provider directly. Such interactions may include entering data into a web-based self-service tool or providing information directly to customer service representatives from the service provider. Similarly, personal information flows directly from EEA affiliates to service providers when the EEA affiliate uploads personal information relating to employees directly onto a service provider's system, which may occur for centralized hosting of employee data or for benefits service providers.

Often, once a main service agreement is signed, the U.S.-based parent then provides an initial set of data to the service provider's system, and subsequently EEA affiliates and the EEA-based employees access the service provider's system and provide data directly to the U.S.-based service provider. For example, a U.S.-based benefits provider enters into a master agreement with a U.S.-headquartered company to provide services globally. Certain employee information is provided by the U.S.-headquartered operations, and subsequently additional personal information is provided to the service provider directly by the EEA affiliates and by individual employees who work for the EEA affiliate. Set forth below is an example showing how personal information flows directly from EEA affiliates or employees of the EEA affiliates to the U.S. service provider.

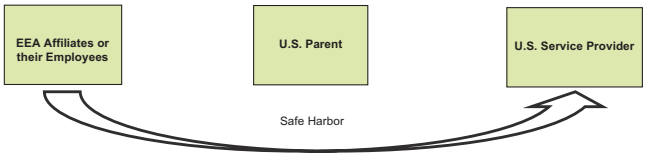


[9] Commission Decision of 27 Dec. 2004 Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (L 385/74), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00740084.pdf.

[10] *Id.* at 5.

  PVLR ISSN 1538-3423

Safe Harbor

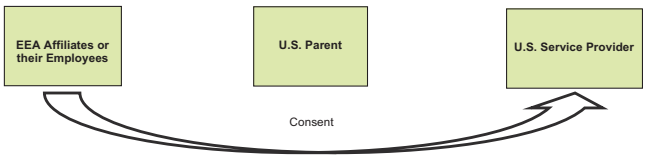


U.S. service providers may elect to be certified by the Safe Harbor. When a service provider has been certified by the Safe Harbor, the service provider is considered adequate by the EC with respect to the cross-border transfer of personal information and must act on the instructions of the EEA affiliate in handling the personal information received from the EEA affiliate pursuant to a data processing agreement.[11]

Just as not all companies using service providers are eligible to be certified by the Safe Harbor, not all U.S.-based service providers are eligible for the Safe Harbor either. Only providers subject to the Federal Trade Commission's and Department of Commerce's jurisdiction qualify at present for the Safe Harbor. Therefore banks, federal branches and agencies of foreign banks, member banks of the Federal Reserve System, and savings and loan institutions are not eligible for the Safe Harbor.

Thus, if an EEA company or its employees provide information directly to a U.S. service provider that has been certified by the Safe Harbor, then the cross-border transfer mechanism obligation is satisfied with respect to the data flowing from the EEA affiliate to the U.S.-based service provider.[12]

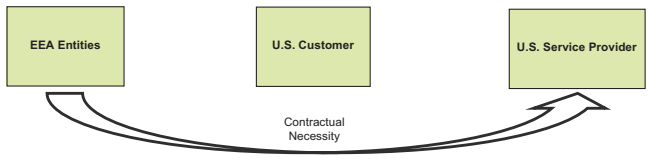
Consent



The EEA affiliate may obtain individuals' consent to permit the transfer of personal information directly from the EEA affiliate to the service provider. Alternatively, the service provider, in the context of providing the service, may obtain individuals' consent on behalf of the EEA affiliate. This often happens in the context of service providers conducting voluntary surveys or providing other services in which employees may elect to participate. In this scenario, consent may be obtained relatively easily because of the direct interaction between the U.S. service provider and the employees based in the EEA, for example through the provider's website/user interface. In order to provide additional safeguards, the U.S. parent may contractually require the U.S. service provider to obtain the consent as part of the service.

Relying on consent, however, may not be practical, depending on the service model being offered. Consent can also be challenging because individuals must be permitted to be able to withdraw their consent at any time. While this ability to rescind consent strengthens the argument that individuals have genuine free choice, it also weakens the effectiveness of consent as a viable option. In many instances however, for example where employee information is shared for benefits purposes, employees will have little to no incentive to withdraw consent.

Contractual Necessity



The service provider may receive information when necessary (i.e., ''indispensable'' information) for the performance of a contract with the individual, or for the performance of a contract in the interests of the individual. For example, under this approach, the EEA affiliate may transfer information to payroll and benefits providers directly when necessary to provide benefits and compensation for employees. Information may also be transferred when it is necessary for investments undertaken for individuals, or required for direct deposits or bank transfers on behalf of the individual.

In an opinion issued in 2005, the EEA data protection regulators stated that in order to rely on the contractual necessity approach, a close and substantial connection between the individual or the individual's interests and the purposes of the contract is required.[13] The opinion stated that no such connection existed, for example, where an international group centralized or outsourced its payment and human resources functions.[14] For these projects, there was no sufficient ''direct and objective link'' between the employees and the data transfers.

The opinion also examined stock option schemes involving transfers to U.S.-based financial service providers. Here the regulators stated that the contractual necessity test may be met, provided that the sets of data transferred and access rights were limited to what was strictly required for the stock option scheme.[15] Transfers required to provide an employee with benefits (which are clearly for the benefit of the employee based in the EEA) are another example of a situation in which contractual necessity is likely to legitimize the transfer of personal information of employees in the EEA to a service provider in the United States.

Thus, for certain types of services which are essential to a contractual relationship beneficial for the indi-

[11] *See* U.S. Dep't of Commerce, *FAQ—Article 17 Contracts*, *available at* http://export.gov/safeharbor/eu/eg_main_018382.asp.

[12] Although personal information will be covered by the Safe Harbor when it is being handled by a U.S.-based service provider, the U.S.-based service provider will not be able to rely on an onward transfer agreement with the U.S.-based parent because the U.S.-based parent is not acting as an agent to the service provider. *See* Safe Harbor ''onward transfer'' principle, *supra* note 6.

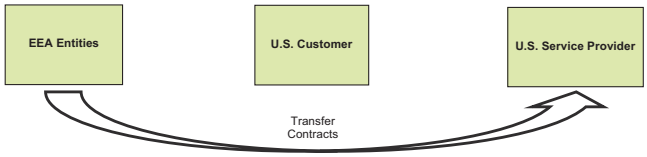
[13] Article 29 Working Party, *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 Oct. 1995*, WP114 (Nov. 25, 2005), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf (4 PVLR 1495, 12/12/05).

[14] *Id.* at 13.

[15] *Id.* at 14.

vidual, contractual necessity can serve to legitimize the cross-border transfer of personal information.

Transfer Contracts



EEA entities may also enter into Standard Contractual Clauses directly with service providers. In 2010, the EC issued a new set of Standard Contractual Clauses to legitimize the transfer of personal information to service providers outside the EEA (''Controller to Processor'' clauses).[16] The Controller to Processor clauses reflect the reality that organizations subcontract to outside service providers.

As with other Standard Contractual Clauses, the substantive provisions of the Controller to Processor clauses cannot be modified. Additional obligations are imposed on the U.S. service provider, particularly if it elects to subcontract to other service providers. For example, the U.S. service provider needs to inform the EEA affiliate of its intention to subcontract all or part of the processing and obtain the EEA affiliate's prior approval. The U.S. service provider would be obligated to enter into a written contract with the subprocessor, which would impose the same obligations on the subprocessor as those of the U.S. service provider, including the incorporation of third-party beneficiary rights against the subprocessor (which would allow individuals to establish contractual claims directly against the subprocessor, but would be limited to the subprocessor's own processing operations). The U.S. service provider must give copies of its contracts with the subprocessor to the EEA affiliate, and the EEA affiliate is obligated to retain and annually update a list of subprocessing agreements. Another substantial drawback of the clauses is the liability imposed on the exporting entity, and that the clauses provide individuals to whom the personal information relates with a direct right of action. Only in environments where the data flow is stable and fairly limited would such limitations work. Also, any amendments to the clauses would need to be approved by all of the information protection authorities in all of the countries from which data are transferred, just as ad hoc contracts would also need to be approved.

The use of Standard Contractual Clauses poses many challenges for companies: It may be difficult to convince a U.S.-based service provider to sign clauses that impose requirements that are imposed by non-U.S. law. Unless the Standard Contractual Clauses are used as-is and unmodified (and are thus not tailored to the company's needs), approval is required from all data protection authorities in the EEA member states from which personal information is transferred. This provides the authorities with the opportunity to scrutinize the appendices to the Standard Contractual Clauses, and request additional details and amendments. Given that there are at least 30 different data protection authorities, this process can be challenging. First, it is very difficult to accommodate all of the authorities in a global arrangement. Second, companies cannot generally seek registration before the contracts are signed by all of the parties. Subsequent changes to accommodate requests from certain data protection authorities could require re-execution—an administrative nightmare. Third, the registration and approval process is very time-consuming, and it may take anywhere from a few days to a couple of years. And, when all of the contracts are signed and registered, the contracts may still need to be updated on a regular basis to reflect the reality of data flows.

Binding Corporate Rules

BCRs would not allow data sharing between EEA affiliates and U.S. service providers without having other adequacy mechanisms in place.

Conclusions

Companies may not be aware that they have several choices to transfer personal information lawfully from the EEA to U.S.-based service providers. Companies often become overwhelmed by the choices relating to cross-border transfers. Information transfers happen with great frequency and speed; transfer mechanisms need to facilitate compliance but should reflect the company's business needs, including rapid access to and sharing of personal information, often via complex data flows. To ensure compliance, it is important to understand the high-level data flow so that the appropriate compliance mechanisms can be implemented. To date, no true one-size-fits-all solution exists for organizations operating globally that wish to comply with all applicable information protection regimes. But there are in fact many methods by which personal information from the EEA can be transferred to U.S.-based service providers. Companies need to consider all available mechanisms, make informed choices, and tailor their compliance actions accordingly. Companies are not limited to a choice of signing Standard Contractual Clauses. Today, any of the methods described in this article can both meet legal requirements and aid a company's business objectives if designed and implemented properly.

[16] Commission Decision of 5 Feb. 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC of the European Parliament and of the Council (L 39/5), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF.

  PVLR ISSN 1538-3423