Bloomberg BNA

Privacy and Security Law Report®

EU Data Protection

Sixty-five companies have adopted final Binding Corporate Rules, nearly half since 2013. The authors analyze why BCRs are a valuable mechanism for international data transfers, closely examine BCRs for data processors and—noting that the European Parliament's final text of the draft EU data protection regulation doesn't explicitly mention BCRs for data processors—explain why they should be legally recognized.

Why Do We Need Binding Corporate Rules? A Look to the Future

By Myriam Gufflet and Anna Pateraki

Binding Corporate Rules (BCRs) have become increasingly important. As of the beginning of 2015, 65 companies have formally adopted BCRs, and the number of BCRs has nearly tripled over the last couple of years.[1] Factors that have helped promote BCRs include the growth of the data-driven economy, industry demand for better data transfer rules and the increased experience and cooperation of regulators. There is also a favorable climate around BCRs resulting from the introduction of BCRs for data processors (effective as of January 2013) and the explicit recognition of BCRs in the draft European Union Data Protection Regulation (Regulation).[2] As of mid-February 2015, six companies had BCRs for data processors approved,[3] while a significant number of other companies were in the process of obtaining approval.

However, the European Parliament's final text on the draft Regulation (from March 2014)[4] does not explicitly mention BCRs for data processors, only for data controllers, which has led to confusion among companies and regulators alike. In this article, we analyze why BCRs are a valuable mechanism for international data transfers. We focus on BCRs for data processors and explain why they should be legally recognized. We also describe the BCR approval process from the perspective of regulators and the experience of the French Commission Nationale de l'Informatique et des Libertés (CNIL).

I. BCRs as a Mechanism for Global Data Protection Compliance

BCRs are internal corporate rules, such as codes of conduct, that govern intra-group data practices in a binding manner. They are intended to cover frequent, large and complex international data transfers. BCRs describe how a company treats and shares personal

[1] See the full list of BCRs, *available at* http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm (the list is regularly updated). The first BCRs to have been approved were those of General Electric in 2005. Although the approval process during the first years was slow, around 30 companies have completed the BCR process since early 2013.

[2] Proposal for a General Data Protection Regulation, COM(2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (11 PVLR 178, 1/30/12).

[3] Align Technology, Atos, Sopra HR Software (ex HR Access), Royal Philips Electronics, Linkbynet and TMF Group.

[4] General Data Protection Regulation (Provisional Draft, P7_TA-PROV(2014)0212) (European Union) (Mar. 2014), *available at* http://bit.ly/1ywCjwH (13 PVLR 444, 3/17/14).

 ISSN 1538-3423

data, how individuals' rights are respected and how liability is managed on a group-wide basis. They require a high level of compliance maturity within a company, including an array of policies and procedures, audits and controls, complaint handling and trainings that ultimately make BCRs more like a comprehensive compliance program than just a data transfer mechanism. In addition, BCRs involve a regulatory approval process that requires time, resources and review, as well as the support of a company's top management and a dedicated BCR team.

1. High-Level Description of BCRs

Under EU data protection law, data transfers outside the EU are prohibited unless the recipient country has officially been recognized by the European Commission as providing an adequate level of data protection,[5] or certain compliance steps are taken.[6] National regulators in the EU (represented by the Article 29 Working Party, or the WP29) regard BCRs as a compliance mechanism to facilitate intra-group data transfers and have developed formal documentation that companies can use for their BCR application.[7] Although originally BCRs were available only for data controllers (i.e., organizations that determine the purposes and means of the data processing), as of Jan. 1, 2013, BCRs also are available for data processors (i.e., organizations that process data on behalf of and under the instructions of data controllers).[8]

BCRs help save localization costs where possible, enhance accountability and build data protection and security into the company's DNA.

The BCR approval process is similar for data controllers and data processors. In a nutshell, a company must formally apply for BCRs with a ''lead'' regulator, draft and submit the necessary documentation and enter into discussions with the data protection authorities (DPAs) (see section II.2, *infra*, on procedural aspects).

Although initially the BCR approval process could take up to five years, today it may take anywhere from six months to two years depending on the complexity of the case, the number of countries involved, the experience of the lead regulator and the responsiveness of the parties involved (applicant and regulators).

After BCRs have been approved by regulators, they must be implemented within the organization in a binding manner. In addition, the organization may have to obtain data transfer approval from local regulators in compliance with local law.[9] The need for such additional regulatory dealings is sometimes difficult to explain to companies. It should be understood from the outset that approval of BCRs is based on approval at the national level, since they are not mentioned in the EU Data Protection Directive.[10] Thus, the approval of BCRs alone cannot replace the satisfaction of local requirements for data transfer approval (similar to how data transfer approval is required in some countries for the use of EU Model Clauses). However, the presence of BCRs significantly streamlines the local data transfer approval process. Regulators (who often are aware of the BCRs in the context of the mutual recognition or cooperation procedure) generally would not deny approval for data transfers based on the approved BCRs; they would typically just examine whether the facts of the transfer are covered by the scope of the BCRs.

2. Benefits for Companies and Regulators

The use of BCRs has a number of benefits for both companies and regulators. For example, companies are able to harmonize their data management and governance processes by applying uniform rules at each location and in a binding manner. In addition, BCRs help save localization costs where possible, enhance accountability and build data protection and security into the company's DNA. Once implemented, BCRs offer flexibility in the launch of new products and services, as they help produce compliant results at an early stage. BCRs also help companies establish relationships with their primary regulator and increase legal certainty regarding the scrutiny that a company will face. Although BCRs were initially attractive mainly to large multinationals, today they can also be suitable for many medium-sized companies. They can offer a competitive advantage on the market and increase the trust of customers and regulators in the privacy practices of the company.

At the same time, BCRs are useful for participating regulators, as they help to promote cooperation and provide experience with complex data flow scenarios in today's global business environment. Through the increased demand of BCRs, regulators seem more educated and ready to understand the needs of the applicant company (see section IV.1, *infra*, on the role of the CNIL).

[5] The full list of adequate countries is available at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

[6] Compliance steps include BCRs, EU Model Clauses and Safe Harbor.

[7] *See* the WP29's BCR documents, *available at* http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/tools/index_en.htm.

[8] WP195 working document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (June 6, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf (11 PVLR 1005, 6/25/12); WP204 explanatory document on the Processor Binding Corporate Rules (Apr. 19, 2013), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp204_en.pdf.

[9] Countries where regulatory data transfer approval is necessary following the BCR approval include, for example: Austria, Belgium, France, Germany (depending on federal state), Italy, Luxembourg, Poland, Spain and Sweden. *See* Working Party document on national filing requirements for authorizations of transfers on the basis of BCRs (Feb. 2012), *available at* http://ec.europa.eu/justice/data-protection/document/international-transfers/files/table_nat_admin_req_en.pdf.

[10] Directive 95/46/EC, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&qid=1424294454356&from=EN.

  PVLR ISSN 1538-3423

3. The Limits of EU Model Clauses and Safe Harbor

Although for years companies have relied on other data transfer mechanisms such as EU Model Clauses[11] and the U.S.-EU Safe Harbor framework (Safe Harbor),[12] it appears that these mechanisms have certain limitations and that they cannot always efficiently cover the needs of complex company groups. EU Model Clauses have proven difficult to administer within a group of companies for several reasons. For example, while they can easily cover uncomplicated data transfers from company A to company B, they are difficult to implement where a large number of players or subcontractors are involved. Further, EU Model Clauses may lead to lengthy negotiations and burdensome administration, and may require a large number of contracts to be produced. In addition, they may need regular renewals and amendments whenever the details of the data processing change, including updating notifications with or obtaining the approvals of regulators. Quite often they are also difficult to enforce in practice, such as when they are signed by the same executive on behalf of a number of entities within the group.

Following the Snowden revelations in 2013, Safe Harbor was criticized on a political level for allegedly allowing extensive access to EU data by U.S. law enforcement authorities.

At the same time, Safe Harbor primarily covers data transfers to U.S. self-certified organizations, so it does not provide a solution for global data transfers. Although possible reliance on Safe Harbor for onward transfers outside the U.S. should not be excluded, this ultimately requires a case-by-case analysis and careful implementation. For example, factors to be taken into account include whether the onward recipient organization acts as a data controller or as a data processor, whether it is located outside the U.S. and whether additional onward transfer agreements must be concluded.[13] At time, regulators may favor EU Model Clauses that are signed directly between the EU controller and the non-U.S./non-EU onward recipient, such as a service provider, if that recipient was initially known to the EU controller. This may be seen as a rather restrictive interpretation of the Safe Harbor onward transfer principle, but regulators favor it with a view to avoiding Safe Harbor's use to cover data transfers that in reality are direct transfers from EU controllers to non-U.S. recipients. This point has been included in the recommendations of the WP29 to the European Commission in the context of the upcoming changes to the Safe Harbor framework.[14]

However, the limitations of Safe Harbor are not only of a legal nature. Following the Edward Snowden revelations in 2013, Safe Harbor was criticized on a political level for allegedly allowing extensive access to EU data by U.S. law enforcement authorities and the European Parliament asked for it to be suspended.[15] Similar statements were issued in Germany, and regulators there threatened to suspend data transfers to the U.S. based on Safe Harbor until the German government looked into the law enforcement revelations.[16] However, the European Commission has defended the existence of Safe Harbor and suggested 13 improvements to be negotiated with the U.S.[17] The WP29 sent its own recommendations to the European Commission in order to enhance the level of protection afforded by Safe Harbor.[18] Following the criticism, the U.S. Federal Trade Commission (FTC) increased its enforcement of Safe Harbor violations at the beginning of 2014,[19] but some improvements, in particular with regard to national security, are still under discussion between the U.S. and the European Commission, with the objective to finalizing the discussions by the end of May 2015.[20] However, the criticism of Safe Harbor is not new. In the past, German regulators have been vocal in their opposition to Safe Harbor, criticizing issues such as poor implementation by companies or poor enforcement by the FTC, and have urged companies to perform due diligence on recipients' Safe Harbor compliance.[21]

[11] The EU Model Clauses are available at http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.

[12] Information on the Safe Harbor is available at http://export.gov/safeharbor/.

[13] For a detailed analysis, *see* Christopher Kuner, *Onward Transfers of Personal Data Under the U.S. Safe Harbor Framework*, 8 Bloomberg BNA Privacy & Sec. L. Rep. (Aug. 17, 2009) (8 PVLR 1211, 8/17/09).

[14] *See* letter from the WP29 (Apr. 10, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_the WP29_to_ec_on_sh_recommendations.pdf.

[15] *See* European Parliament resolution of 12 March 2014 on the U.S. NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, P7_TA(2014)0230 (Mar. 12, 2014), *available at* http://bit.ly/1LwfNve.

[16] *See* German Conference of Data Protection Authorities Press Release, *Conference of data protection commissioners says that intelligence services constitute a massive threat to data traffic between Germany and countries outside Europe* (July 24, 2013), *available at* http://bit.ly/1AmjYXC.

[17] For the European Commission's 13 recommendations on Safe Harbor, *see* European Commission Memo, *Restoring Trust in EU-US data flows - Frequently Asked Questions*, (Nov. 27, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

[18] *See* the WP29 Letter to Viviane Reding, Vice President and Commissioner for Justice, Fundamental Rights and Citizenship, European Commission (Apr. 10, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_the WP29_to_ec_on_sh_recommendations.pdf.

[19] *See, e.g.*, FTC Press Release, *FTC Settles with Twelve Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework* (Jan. 21, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply.

[20] As announced on Jan. 21, 2015 by Vira Jourová, Commissioner for Justice, Consumers and Gender Equality, before the EU Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE), *available at* http://bit.ly/1zAnon2 (around 14:25:00).

[21] *See* 2010 resolution of the German data protection authorities (Apr. 2010), *available in German at* http://bit.ly/1EtP5RM; Press Release, German data protection authorities,

At this point it should be made clear that Safe Harbor is still in effect, as it is based on a valid European Commission adequacy decision. However, its credibility has been damaged in the EU, and will require substantial effort from both EU and U.S. officials to rebuild. It remains to be seen how the upcoming changes to Safe Harbor will impact its position as a global data transfer mechanism. Given the existing uncertainties around Safe Harbor and the practical limitations of EU Model Clauses, companies continue to seek suitable and sustainable solutions for intra-group data transfers.

4. Explicit Recognition of BCRs for Processors

Although BCRs have now been in effect for almost a decade, they are not codified under the EU Data Protection Directive. This has led to a number of problems, such as legal constraints for some EU regulators to recognize BCRs as a mechanism for international data transfers or to participate in the BCR mutual recognition procedure.[22] The draft Regulation aims to put an end to those problems and explicitly recognize the use of BCRs as a legal mechanism for data transfers.[23] The European Commission's proposal (from January 2012) explicitly recognized the use of BCRs for both ''the controller's or processor's group of undertakings.'' The WP29 issued a paper on BCRs for processors in June 2012 (effective as of Jan. 2013), notably six months after the draft Regulation was published, which shows that the recognition of BCRs for processors was being prepared within the EU institutions for a significant amount of time (in fact, since 2010) and therefore represent a long-awaited achievement.

However, the final position of the European Parliament (from March 2014) suggested removing the reference to data processors and replacing it with wording recognizing BCRs only for the ''controller's group of undertakings and those external subcontractors that are covered by the scope of the binding corporate rules,''[24] while keeping processors in the definition of ''binding corporate rules.''[25] This proposed wording has created confusion and raised questions as to its actual meaning, as well as whether regulators would be legally obliged to accept and recognize BCRs for data processors if it is not codified in the Regulation. One should note that the European Parliament's text neither contains a clear justification as to the deletion of the explicit recognition of BCRs for data processors nor discusses the numerous amendments that members of the European Parliament tabled back in spring 2013.[26]

Prior to the final vote, the WP29 reacted to the European Parliament's concerns and supported the BCRs for data processors by stating:

> [t]he Regulation provides for an enlarged role for processors in ensuring adequate data protection and also considering the introduction the accountability principle, [. . .] BCRs for processors are a valuable tool in ensuring adequate protection when transferring data and should therefore not be deleted. BCR for processors provide for an obligation of information toward the controller that all subprocessors' activities, which allows him or her to object to any new sub-processing and to duly inform the data subjects. The Standard Contractual Clauses of 2010 also cover this situation.[27]

BCRs for data processors are a valuable tool for increasing accountability and should not be the victim of skepticism around law enforcement access.

In June 2014, this statement was renewed by the WP29, which sent a letter to EU institutions to promote BCRs for data processors in the context of the trialogue on the draft Regulation.[28]

Although the Council's position has not yet been finalized, ''partial general agreement'' on data transfers was reached in the Justice and Home Affairs Council meeting of June 5–6, 2014. The Council of the EU does not seem to share the European Parliament's view regarding BCRs for data processors. In the recap text of the Greek Presidency (from June 30, 2014), the wording used by the Council was intended to cover a ''group of undertakings or group of enterprises engaged in a joint economic activity.''[29] However, data processors were referenced later in the text of the Regulation (Article 43(2)(f)) and therefore the recognition of BCRs for processors, although blurred, remained valid. During the discussions on this text under the Greek Presidency, some countries expressed reservations regarding this wording, while others, such as Belgium, wondered ''why the reference to controller's or processor's group

Conference of data protection commissioners says that intelligence services constitute a massive threat to data traffic between Germany and countries outside Europe (July 24, 2013), *available at* http://bit.ly/1AmjYXC.

[22] BCRs are not recognized in Hungary and Portugal. In Bulgaria, although the national law does not explicitly recognize BCRs, the Bulgarian regulator may authorize transfers covered by BCRs on a case-by-case basis. In Poland, amendments to the Polish Data Protection Act (effective as of Jan. 1, 2015) explicitly recognize BCRs. The amendments are available in Polish at http://orka.sejm.gov.pl/proc7.nsf/ustawy/2606_u.htm, Art. 9 (14 PVLR 211, 2/2/15).

[23] Draft Regulation at Article 43.

[24] *See* General Data Protection Regulation (Provisional Draft, P7_TA-PROV(2014)0212) (European Union) (Mar. 2014), Article 43(1)(a) and (f), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN.

[25] *Id.*, Article 4(17).

[26] *See* table amendments Nos. 2469–2473 (where references to ''processors'' are made) (Mar. 6, 2013) *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/am/929/929519/929519en.pdf (12 PVLR 524, 3/25/13).

[27] *See* Comments of the WP29 to the LIBE vote of Oct. 21, 2013, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131211_annex_letter_to_greek_presidency_the WP29_comments_outcome_vote_libe_final_en_.pdf.

[28] *See* Letter from the WP29 to Martin Schultz, President of the European Parliament (June 12, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140612_the WP29_bcr-p_general_ep_president.pdf.

[29] *See* Note from Greek Presidency Working Party on Information Exchange and Data Protection (June 30, 2014), *available at* http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011028%202014%20INIT.

  PVLR ISSN 1538-3423

of undertakings was deleted'' and wanted to support the possibility of giving explicit legal recognition to Processor's BCR.[30] Therefore, this point will likely be debated further during the legislative process.

Following the Snowden revelations, the European Parliament has taken the approach of restricting international data transfers because of concerns about law enforcement access. However, it should be understood that BCRs for data processors are a valuable tool for increasing accountability and should not be the victim of skepticism around law enforcement access. In particular, BCRs for processors provide transparency for the data controllers and the EU regulators in case of law enforcement access, with a similar effect as Article 43(a) of the Regulation that the European Parliament inserted in its final position (from March 2014). It should be noted that neither BCRs nor Safe Harbor nor EU Model Clauses were designed to legitimize law enforcement access, since they were aimed at covering transfers between private actors. In particular, both EU Model Clauses and BCRs include a law enforcement exception for national sovereignty reasons[31] that should be interpreted restrictively and on a case-by-case basis, and cannot legitimize indiscriminate and massive surveillance from third countries.[32] Therefore, law enforcement issues should be dealt with separately at a political level and not result in a weakening of the existing data transfer mechanisms.

II. From Traditional BCRs to BCRs for Data Processors

We analyze below the view of regulators with regard to some of the key aspects of BCRs for data processors and how they relate to BCRs for data controllers (BCR-C). Regulators have leveraged many of the concepts behind traditional BCRs to prepare for BCRs for data processors (BCR-P). Some of the concepts of BCRs for processors are also inspired by concepts included in EU Model Clauses for controller-to-processor data transfers.

1. Key Issues

a. Binding nature

As in the case of traditional BCRs, the binding nature of BCR-P is the cornerstone of such mechanisms, as it falls within the scope of the derogation provided for in Article 26(2) of the EU Data Protection Directive, under which data transfers to third countries can be authorized providing that ''*the controller adduces adequate safeguards*.''[33] Hence, in order to provide such ''*adequate safeguards*,'' BCR-P will be made binding internally (i.e., upon the group's entities and their employees), which means they are obliged to comply with the group's BCR-P. In addition, BCR-P will be made binding externally (i.e., upon data subjects, controllers and EU DPAs), which should be understood in terms of the enforceability of the BCR-P (see section II.1.e, *infra*).

The criteria suggested by the WP29 to ensure the binding nature of the rules for entities and employees is the same as the criteria already suggested for BCR-C.[34] The criteria chosen by the applicant will be explained in its BCR-P application form.[35]

Therefore, group entities may be bound, for instance, by the signature of an intra-group agreement; the incorporation of the BCR-P into the group's general business principles, backed by appropriate policies, audits and sanctions; and/or by a unilateral declaration or undertaking made or given by the parent company that is binding on the other group members.[36]

BCR-P are specifically aimed at covering situations involving multi-party sub-processing by a processor acting on behalf of a controller.

Employees must be aware of, understand and apply the BCR-P. In practice, this means that they will (i) be informed of the BCR-P's implementation within their organization; (ii) be compelled to comply with the BCR-P, for instance, through their work employment contract and/or collective agreements; (iii) be made aware that failure to comply with the BCR-P may lead to disciplinary sanctions; and (iv) be trained on the BCR-P.[37] Thus, internal bindingness is the first step to

[30] *See* Note from Greek Presidency to COREPER/Council (May 19, 2014), at n.50, *available at* http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209865%202014%20INIT

[31] *See* Controller-to-Processor EU Model Clauses, 2010/87/EU (2010), at Clause 5(d)(i), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=EN (9 PVLR 253, 2/15/10); the WP29 documents on BCRs (for data controllers): WP153, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (2008), § 6.3, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf; WP154, Working Document Setting up a framework for the structure of Binding Corporate Rules (2008), § 16, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_en.pdf (7 PVLR 1059, 7/14/08).

[32] *See* WP228, Working Document on surveillance of electronic communications for intelligence and national security purposes (2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf.

[33] *See* Directive 95/46/EC, Article 26(2), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:PDF (emphasis added).

[34] For BCR for controllers, *see* WP153, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (2008), § 1.2, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf. For BCR-P, see WP 195, Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (2012), § 1.2, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf (11 PVLR 1005, 6/25/12).

[35] *See* WP195a, Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities (2012), Part II.4, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195a_application_form_en.doc.

[36] Note that unilateral declarations or undertakings may not be accepted by regulators in some EU Member States that will require a contract to ensure bindingness, pursuant to their legal system.

[37] Training on BCR-P must at least be provided to personnel who have permanent/regular access to personal data, and

ensure that the BCR-P will provide adequate and effective safeguards to personal data that is transferred to third countries.

b. Sub-processors

BCR-P are specifically aimed at covering situations involving multi-party sub-processing by a processor acting on behalf of a controller, which may lead to massive international data transfers, as is usually the case with cloud computing services, for instance.

The use of sub-processors may lead to different obligations, depending on whether the sub-processor is part of the group or is external.

In both cases, sub-processing can only be completed after obtaining the controller's written consent.[38] According to the WP29, consent may be general (i.e., given by the controller at the beginning of the service) or specific (i.e., required for each new sub-processor). When the parties agree to a general consent, the processor will inform the controller of any intended changes concerning sub-processors in such a timely fashion that the controller has the opportunity to object to the change or to terminate the contract before the data are communicated to the new sub-processor.

Where the sub-processor is not part of the group (or is part of the group but is not bound by the BCR-P), additional requirements must be met in order to comply with the confidentiality and data security requirements (Articles 16 and 17 of the EU Data Protection Directive). To that extent, a written agreement must be signed with that sub-processor, stating that data are only processed under the controller's instructions and that appropriate technical and organizational measures are adduced to protect the data that are sub-processed. In addition, the written agreement must impose upon the sub-processor the duty to comply with some of the obligations imposed on the BCR-P (e.g., creation of third-party beneficiary rights for data subjects,[39] responsibility of the controller,[40] cooperation duty[41] and data protection safeguards[42]). Finally, if the sub-processor is located outside of the European Economic Area (EEA), adequate safeguards must be provided to protect the personal data transferred, as required by Articles 25 and 26 of the EU Data Protection Directive.

c. Duty of cooperation

Another key component of BCR-P is the duty to cooperate with DPAs and controllers.

- *Cooperation with DPAs*:[43] This cooperation duty does not differ from the duty provided for in BCR-C. That said, such a general duty will likely fall into one of three categories:
  i. advice (i.e., compliance with the advice of the competent DPAs on any issues related to BCR-P);
  ii. information (e.g., updates,[44] audit reports,[45] conflict of laws[46] and law enforcement requests[47]); and
  iii. audit (the DPA competent for the controller is empowered to audit the group entities and external sub-processors if required and legally possible).
- *Cooperation with controllers:* Aside from the processor's duty to comply with the instructions given by the controller regarding data processing, processors and sub-processors must cooperate with and assist the controller to comply with their legal duties under data protection law in order to be well positioned to respond to requests from data subjects or DPAs (including investigations). This must be done in a reasonable timeframe and to the extent reasonably possible.

  In concrete terms, it means they will provide the controller with any information that would be necessary for the controller to know, in particular concerning any change of sub-processors, updates to the BCR-P, complaints received from data subjects, audit reports, conflict of laws or law enforcement requests.

  In addition, this cooperation duty implies that the processor helps and assists the controller while processing personal data in order to comply with the basic data privacy principles: transparency and fairness, purpose limitation, data quality, security, data subjects' rights, sub-processing within the group and onward transfers to external sub-processors.

  Finally, it should be noted that outsourcing of data processing operations must not induce for the controller a loss of monitoring over the data processed on its behalf. To that extent, the processor and its sub-processors (internal and external) will agree to submit their data processing facilities to audits, either carried out by the controller or by an independent third party chosen by the controller.

d. Liability

Another key component of BCR-P is the liability toward data subjects and data controllers.

- *Toward data subjects:* Where a data subject suffers harm caused by a breach of the BCR-P by the processor or any of its sub-processors (internal or external), he/she will have enforcement rights

---

who are involved in the collection of personal data or in the development of tools used to process personal data. *See* WP195, § 2.1.

[38] *See* WP204, Explanatory document on the Processor Binding Corporate Rules (2013), § 2.2, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp204_en.pdf.

[39] WP195 § 1.3.

[40] *Id.* at § 1.4.

[41] *Id.* at § 3.

[42] *Id.* at § 6.

[43] *Id.* at § 3.1.

[44] *Id.* at § 5.1: DPAs must be informed of any modifications to the BCR-P, and any substantial changes to the BCR-P and/or to the list of bound entities must be reported once a year to the competent DPAs, with a brief explanation of the reasons justifying the update.

[45] *Id.* at § 2.3: The DPA competent for the controller shall have access to audit reports upon request.

[46] *Id.* at § 6.3: The DPA competent for the controller shall be informed that the existing or future legislation applicable to a group member may prevent it from fulfilling the controller's instructions and/or its obligations under the BCR-P and/or the service agreement.

[47] *Id.*: The DPA competent for the controller and the lead DPA for the BCR-P should be clearly informed of any request for disclosure made by a law enforcement authority.

  PVLR ISSN 1538-3423

against the processor if it is not possible to act against the controller.[48] Such third-party beneficiary rights cover judicial remedies, as well as the right to receive compensation for any damage suffered.

The processor will appoint an entity that will bear liability for all the other members of the processor's group in case of a breach of the BCR-P or of the written agreement signed with external sub-processors pursuant to Article 17 of the EU Data Protection Directive. It may choose between the EU headquarters or the EU member with delegated data protection responsibilities. If this proves difficult, for instance because of the group's organization, DPAs may agree that each EU processor that exports data will be liable for its own breaches and those committed by the data importer of any subsequent sub-processor.

- *Toward data controllers:* In addition to the liability toward data subjects, the processor is liable toward its customers acting as data controllers. Therefore, in the event of a breach of the BCR-P, of the service agreement or of the written agreement signed with external sub-processors, the controller can lodge a claim against the entity at the origin of the breach.

  Where the latter is an entity of a non-EU processor or of a non-EU external sub-processor, the controller should be entitled to act against the entity that has accepted liability (EU headquarters, EU member with delegated data protection responsibilities or EU processor that exports data).

e. Enforceability

One consequence of the fact that entities and employees must comply with the BCR-P is that data subjects, controllers and DPAs can take action in the event of an infringement of the BCR-P, the service agreement or the written agreements signed with external sub-processors.

- *Data subjects:* As explained above, data subjects are given third-party beneficiary rights that they can enforce. These rights are listed by the WP29[49] and cover, for instance, the fact that data subjects will be given easy access to the BCR-P or the processor's duty to process data under the controller's instructions.

  When a breach has occurred, data subjects may lodge complaints before the competent DPAs or bring action before the court of their choice among the jurisdiction of (i) the EU headquarters, (ii) the EU member with delegated data protection responsibilities or (iii) the EU processor that exports data (i.e., the group's member at the origin of the transfer). If no member of the processor's group is located in the EU, data subjects may lodge claims before the court of their residence. However, if other jurisdictional rules are more favorable for data subjects under applicable national law, they would apply.

  Finally, it should be noted that the burden of proof lies with the processor, not the data subject. In practice, this means that where a data subject can demonstrate he/she has suffered damage and establish facts showing that it is likely that the damage has occurred because of the breach of BCR-P, the member of the group that has accepted liability must prove that the non-EU member of its group or the external sub-processor was not responsible for the breach of the BCR-P giving rise to those damages or that no such breach took place. Therefore, if the entity that has accepted liability can prove that the member of the group outside the EU is not responsible for the breach, it may discharge itself from any responsibility.

- *Data controllers*: In the same spirit as third-party beneficiary rights for data subjects, controllers are also entitled to enforce the BCR-P, the service agreement or the written agreements signed with external sub-processors in the event of a breach. In addition, the burden of proof rules are the same as those for data subjects.

- *Data Protection Authorities:* In case of a breach of the BCR-P, the DPAs competent for the controller could withdraw the approval they previously granted to the controller on the basis of the BCR-P.

  Moreover, insofar as DPAs have the duty to monitor international data transfers, they have the power to investigate, sanction and engage in legal proceedings in case of non-compliance.

2. Procedural Issues

a. Similar procedure as known today for controllers

In order to constitute an admissible legal basis for data transfers, the BCR-P will be reviewed by the DPAs concerned by the transfers. Therefore, if an applicant intends to transfer data from all of the EEA countries, it means that the 31 EEA DPAs acknowledge that the applicant's BCR-P provide adequate protection for the data transferred.

The procedure is the same as the one for BCR-C and a mechanism of mutual recognition was created to speed up the procedure, which is detailed below. In terms of length, it varies from one application to another and depends on the reactivity of all parties.[50]

b. DPA approval and cooperation of regulators

Approval by the DPAs means that they recognize that the BCR-P of a group provide sufficient safeguards to protect personal data transferred, on the basis of which the processor's customers, acting as controllers, will be

[48] This applies if the data controller has factually disappeared or has ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the data controller by contract or by operation of law.

[49] *See* WP204, § 2.3.3.1.

[50] A recent internal audit carried out by the WP29 showed that on average, it takes around 7.5 months for companies to amend the BCR-C/P to take into account the DPAs' comments; around 5 months for the lead DPA (review of the first drafts and coordination with the other DPAs); and 3 to 3.5 months for the other DPAs (co-reviewers and DPAs not part of the mutual recognition procedure).

able to rely to transfer data to third countries and obtain the necessary national transfer authorizations before the competent DPAs.

The BCR-P approval procedure can be divided into six steps, as detailed below:

- *Choice of a lead DPA:* First, the applicant will choose a lead DPA (usually the DPA of a company's European headquarters), the mission of which will be to review the BCR-P, assist the applicant and coordinate the procedure with the other DPAs. Such choice should be based on factual criteria listed in the application form,[51] linked to the specific situation of the applicant.[52] This choice must be agreed upon by the other DPAs concerned by the transfers, which—after receipt of Part I of the application form—have 15 days to object (this very rarely happens).

- *Review by the lead DPA:* Once the choice of the lead DPA is validated, the applicant will provide the lead DPA with at least: (i) the application form; (ii) the draft BCR-P; (iii) examples of audit and training programs; and (iv) any documentation that would be useful to understand how the BCR-P will be implemented within the group's applicant. Then, the lead DPA will review the draft BCR-P against WP195 and provide comments to the applicant, which should be taken into account. In practice, it usually takes more than one draft and more than one review to reach a draft that satisfies both parties. When the lead DPA is satisfied, the draft BCR-P is sent to two other DPAs, called ''co-reviewers.''

- *Review by two co-reviewers:* The role of the co-reviewers is to perform a ''quality'' review against WP195 within one month. There is no set criterion to choose a co-reviewer. In most cases, the lead DPA asks the applicant if it has any preferences (for example, due to the location of an important entity). But in any case, the legal value of the review will be the same for a DPA of a country where the applicant has little activity and for a DPA where the applicant is much more active.

  The co-reviewers may request some amendments from the applicant, which must take them into account. In practice, occasionally DPAs do not have any comments, while other times they may require modifications. In 2013, the WP29 took measures to speed up the procedure, and decided that when a co-reviewer has not given any feedback on the draft BCR or requested any deadline extension, the lead DPA would interpret this to mean that the co-reviewer does not have any comment.

  Once both co-reviewers are satisfied with the draft BCR-P, the document will follow two parallel routes: the mutual recognition procedure and the co-operation procedure.

- *Mutual recognition procedure:* This procedure consists of a network of DPAs in the EEA that have agreed to automatically recognize BCRs in their countries—once they have been approved by the lead regulator and two co-reviewer regulators—without further involvement from the applicant company. It was created by the WP29 in 2009 and has greatly reduced the length of DPAs' reviews. Its principle is that the DPAs that are part of this procedure (21 EEA DPAs as of February 2015[53]) will rely on the reviews made by the lead DPA and the two co-reviewers. Therefore, they will not review the draft and will only acknowledge safe receipt of the BCR-P. The lack of participation by a regulator in the mutual recognition network may be related to local law constraints and might not necessarily mean that a regulator does not favor the use of BCRs.

- *Cooperation procedure:* The other DPAs (10 as of February 2015[54]) that do not participate in the mutual recognition procedure will receive the draft BCR-P and have one month to review it and provide any comments. In practice, it is relatively rare that amendments are required at this stage. When the lead DPA does not receive any response from these DPAs once the deadline has passed, it concludes that the other DPAs do not have any remarks on the draft BCR-P.

- *Closure of the procedure:* Once the one-month deadline is past, provided that none of the other DPAs have requested modifications, the lead DPA can notify all of the DPAs that the procedure has been closed. A letter from the lead DPA's chair will be sent to the applicant to formalize the ending of the procedure.

We would like to note that cooperation between DPAs does not only work through BCR approval procedures, but also through the WP29, which consists of DPAs and drafts opinions and/or working documents on the matter and shares experiences to ensure harmonization between DPAs.

c. New procedure suggested by the EC in the draft Regulation

The draft Regulation provides for a different approval mechanism, based on the ''consistency mechanism,''[55] to enhance cooperation between DPAs.

- In the version of the draft Regulation issued in January 2012 by the European Commission (EC), the consistency mechanism in the context of BCRs would function as follows (however, this might change during the legislative process):

[51] *See* WP195a, op. cit. n2.

[52] For instance, location of the group's EEA headquarters, location in the EEA of the group's entity with delegated data protection responsibilities, etc.

[53] Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Estonia, France, Germany, Iceland, Ireland, Italy, Latvia, Liechtenstein, Luxemburg, Malta, the Netherlands, Norway, Slovakia, Slovenia, Spain and the United Kingdom are part of the mutual recognition procedure. This list, along with more information on the mutual recognition procedure, is available at http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm.

[54] Croatia, Denmark, Finland, Greece, Hungary, Lithuania, Poland, Portugal, Romania and Sweden are part of the cooperation procedure. However, Poland is likely to participate in the mutual recognition in the future due to changes to the Data Protection Act, effective as of Jan. 2015.

[55] Articles 59 and 60 of the draft Regulation.

  PVLR ISSN 1538-3423

i. the competent DPA (the one of the controller's main establishment[56]) will inform the chair of the European Data Protection Board (EDPB, which will be the successor of the WP29) of the measure it intends to take and any necessary information;

ii. the chair will transfer this information to the EDPB members and the EC, and the EDPB will decide within one week, by simple majority, whether it is necessary to issue an opinion on the matter;

iii. the EDPB opinion will be adopted within one month by simple majority;

iv. in the meantime, the EC may adopt an opinion within 10 weeks of communication of the information;

v. the competent DPA will take into account the EDPB's and EC's opinions and will inform the latter within two weeks whether it will maintain its draft measure or amend it to take the opinions into account. In the second case, it will also communicate the amended version; and

vi. if the competent DPA maintains its draft measure and the EC continues to have serious doubts regarding the draft measure, it may adopt a decision within one month requiring the competent DPA to suspend the measure for up to 12 months while it tries to reconcile the position or adopt a measure of its own.

- There are some potential issues under the EC's proposal, such as the following:

i. The new BCR approval procedure proposed by the EC (which will apply not only for BCRs, but also for any measure that would concern more than one DPA) suggests a mechanism aimed at expediting BCR approvals. However, not only is the function of this mechanism difficult to understand, but the time frames set up for the EDPB to draft and adopt an opinion seem too short given the nature of the matter (i.e., the review of draft BCRs). Nevertheless, the European Parliament removed these time frames from its version of the draft Regulation (as of March 2014).

ii. In addition, the EC is given too powerful a role, since it is the only party with the power to act against a measure that a competent DPA intends to take; the EC therefore has an exclusive competence toward a matter even where it concerns several DPAs. This provision has been deleted by the European Parliament.

iii. Finally, as currently drafted, the efficiency of the consistency mechanism is questionable for BCRs, as the mechanism will give the 28 Member States the opportunity to comment on the draft BCRs. In contrast, the current system of mutual recognition was created to avoid this situation.

3. Differences from the BCRs for Controllers

In terms of content, there are many similarities between BCR-C and BCR-P, and the differences are explained by the fact that BCR-P cover data processed and transferred by a processor's group (i.e., on behalf of and under the instructions of a customer acting as data controller). There are four main differences:

a. *Third-party beneficiary rights*: As for BCR-C, data subjects will be given beneficiary rights through the inclusion of a third-party beneficiary clause within the BCR-P, which means they are entitled to enforce compliance with the BCR-P against the controller by lodging a claim before the competent DPA or a court competent for the EU controller. However, if this proves impossible,[57] data subjects may take action against the processor.[58]

b. *Cooperation with controllers*: In addition to its duty to cooperate with DPAs, the processor's group will commit to cooperate with its customers acting as controllers. This means that all entities of the group and their employees will respect the controllers' instructions regarding the processing and the security and confidentiality measures, and will cooperate and assist the controllers in order for them to comply with data protection laws. This can be achieved, for instance, by providing the controllers with any information that would be relevant to handle complaints or respond to inquiries or investigations from a competent DPA.

c. *Privacy principles:* BCR-P must contain a clear commitment of the processor's group to help the controller comply with the core data protection principles, such as transparency and fairness, purpose limitation, security and onward transfers.

d. *Law enforcement requests*: In addition to the commitment to notify the processor of the existence of applicable legislation that may prevent it from complying with the BCR-P and/or the controller's instructions, the BCR-P must contain a commitment to inform the controller of any legally binding request for disclosure received from a law enforcement authority (unless prohibited), to put the request on hold and inform the DPA competent for the controller and the lead DPA for the BCR-P of the request. This information process does not aim to legitimate the transfer to the law enforcement authority, which will still rely on a legal basis according to the applicable law.[59] This provision is close to Article 43(a) introduced in the draft Regulation by the European Parliament.

III. How Best to Approach a BCR Project

Organizations often contemplate how best to approach a BCR project at its early stages and whether to apply for BCR-C, BCR-P or both. The introduction of BCRs for data processors has opened the door for many service providers/data processors to apply for BCRs, but the same organizations may act as data controllers for

[56] Article 51 of the draft Regulation.

[57] *See* n.46, *supra*.

[58] See part II.1.e, *supra*.

[59] *See also* WP228; WP211, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (Feb. 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

other data processing activities (e.g., HR management and marketing). In addition, there are sometimes complex business models where the distinctions between controller and processor may be blurred and the organization may have difficulties deciding which BCR model to apply for.

Various options are possible. For example, organizations that already have BCRs for controllers in place (e.g., for HR processing) can also apply for BCRs for processors (e.g., for their core business processing). In this case, they can leverage their existing experience with BCRs and extend it within the group to cover other entities in their capacity as data processors and their internal subcontractors. In other instances, organizations without BCR experience may choose to apply for both BCR models simultaneously (as described below), or for just one of them, depending on the goal they wish to achieve. Generally, the preparation needed for one of the BCR models can be leveraged for the other BCR model.

In addition, organizations considering BCRs should assess whether their existing data practices (or policies and procedures) offer a strong base to build on or whether additional work should be completed before applying for BCRs. This is particularly relevant for organizations that have relied on other data transfer mechanisms (e.g., EU Model Clauses, Safe Harbor) but are now considering a transition to BCRs for all or part of their global data flows.

BCRs only cover intra-group data transfers and therefore are not universal remedies.

As a first step, an organization seeking to benefit from BCRs should have a clear view of the data flows and the entities involved, assess the role and responsibilities of those entities and define the scope of the intended BCRs (e.g., geographic locations, types of processing activities). With regard to the processing activities that would not be covered by the BCRs, the organization should assess whether there is a need for additional data transfer mechanisms. The approach that works best for each organization may vary depending on the level of compliance maturity within the group, the company structure and how it manages risk.

However, BCRs only cover intra-group data transfers and therefore are not universal remedies. An organization may have to develop or review its strategy for handling data transfers to non-members of the group since non-members would not be bound by the BCRs. For example, the organization should assess whether additional contracts should be implemented to cover non-member recipients. In the case of BCRs for processors, internal subcontractors are covered by BCRs, but additional contracts should be implemented with external subcontractors. There have also been discussions at the political level regarding how to facilitate data transfers between groups of companies where each has implemented its own BCRs; however, it is too early to know how this idea will be developed in the future.

IV. The View of Regulators

1. The Role of the CNIL Regarding BCRs

The CNIL has been involved in BCRs since 2008 and the WP29 had BCRs as a priority topic for 2008/2009.[60] In this regard, representatives of the CNIL regularly speak at international conferences to promote and explain BCR mechanisms. In addition, the CNIL is the coordinator of the WP29 international transfers subgroup, which is responsible for designing the WP29's doctrine on BCR-C/P.

For the CNIL, BCRs tend not to be just transfer tools but rather genuine compliance and governance programs, as they define the group's worldwide core values on personal data protection as well as accountability measures to ensure in practice that BCRs are complied with.

In such context, it seemed obvious for the CNIL that a dedicated BCR Unit join the Directorate for Compliance in the context of the reorganization of the CNIL's structure in April 2014. The main missions of the CNIL's BCR Unit are promoting BCRs, assessing draft BCRs and Francophone BCRs[61] and coordinating procedures with the CNIL's counterparts. In addition to enhancing the visibility of BCRs and Francophone BCRs, the creation of the CNIL's BCR Unit contributes to reducing the duration of assessing draft BCRs when the CNIL is the lead DPA or co-reviewer. For instance, after the CNIL's BCR Unit was created in 2014, the approval procedure of a draft BCR that had been submitted to the CNIL acting as the lead DPA took only six months, thanks to the responsiveness of the applicant and the CNIL's BCR Unit.

As of the beginning of 2015, the CNIL has been the lead authority for 23 approved BCRs, and is constantly working toward promoting BCRs and raising awareness.

2. How Regulators Work with Companies

The point of contact for BCR applicants is the lead DPA. As a result, one important mission of the lead DPA is to provide assistance to applicants, which translates into offering explanations on the procedure and the WP29 papers and providing guidance on how to meet the WP29 requirements while taking into account the specific characteristics of the group in terms of internal organization, culture and processes.

Then, once the applicant submits its first draft to the lead DPA, the lead DPA will review it against the WP29 documents and provide comments to the applicant. It may take more than one draft and one review to reach a draft that satisfies both parties. In the meantime, the lead DPA is available to discuss issues that the applicant encountered while drafting the BCR.

Finally, the lead DPA coordinates the procedure between all DPAs so the applicant benefits from having a single point of contact instead of having to contact each DPA involved in the BCR review.

[60] On this subject, the WP29 ''BCR toolbox'' (WP153, WP154 and WP155) was adopted in 2008 and the mutual recognition procedure was created in 2009.

[61] *See* Section V.4, *infra*.

  PVLR ISSN 1538-3423

3. What Regulators Expect from Companies

For regulators, the key elements of a successful BCR application with DPAs are based on a ''3C rule:'' cooperation, compliance and clarity.

''Cooperation'' means that applicants will be transparent with the DPAs involved in the review procedure and provide them with any relevant information to understand the structure and the culture of the group, as well as its internal processes. The idea is that DPAs have all the information they need to fully comprehend how BCRs are drafted and how they will be implemented in practice.

''Compliance'' means that the applicant takes into account the WP29's requirements and the principles of the EU Data Protection Directive. The more that BCRs include the terms, requirements and principles from these documents, the less time the review procedure will take.

''Clarity'' means that BCR-C/P are drafted as intelligibly as possible, with a clear and organized structure and without too many documents. If an organization applies for both BCR-C and BCR-P, it is conceivable to put both type of rules in a single document, as long as it is clear when the commitments and processes concern both situations and when they are specific to either BCR-C or BCR-P.

V. Conclusions and Key Trends for the Future

BCRs can be considered the future of international data transfers. They constitute a pragmatic method of integrating data protection into the culture of a company group. In particular, BCRs for data processors deserve to be included in the forthcoming Regulation, as they essentially help promote accountability in a variety of new businesses, and should be legally recognized. Some notable trends regarding the future of BCRs are summarized below.

1. **The Number of BCRs Will Continue to Increase.** More and more companies are expected to select BCRs as their permanent solution for international data transfers. Nowadays, BCRs appeal not only to large corporations, but also to many medium-sized companies. The release of BCRs for data processors will allow a large number of new businesses to benefit, including a variety of service providers and members of the outsourcing industry.

2. **Accountability and Process-Based Compliance Will Take Over.** Companies understand that BCRs are an excellent way of moving away from obsolete and bureaucratic practices. They help enhance accountability and promote compliance at the core of a company's data processes.

3. **Cooperation Among EU Regulators Is Improving.** Because more BCRs are being adopted, regulators will have to work closely with one another, exchange views and gain more experience with complex global data transfer issues. The BCR approval process will run more smoothly and faster in the future.

4. **Interoperability with the Other Compliance Tools Will Increase.** While it may be too early to talk about interoperability between the European and the Asia-Pacific Economic Cooperation (APEC) systems, the WP29 and its APEC counterparts are working together closely to provide practical tools to multinational organizations that do business both in Europe and the Asia-Pacific region and look for global solutions for their data transfers. In March 2014, the WP29[63] and its APEC counterparts published an informal pragmatic checklist for organizations applying for both approval of BCRs in the EU and certification under the APEC Cross-Border Privacy Rules in the APEC region that could serve as a basis for double certification.[64] In addition, the WP29 and its APEC counterparts continue to cooperate and are currently developing case studies that would examine the experience of organizations seeking both BCR approval and CBPR certification. Depending on the outcome of such work, they could decide whether to further develop practical documentation for use by companies.

   Further, the Association of French-Speaking Data Protection Authorities (AFAPDP)[65] adopted in late 2013 a resolution on the framework procedure for personal data transfers within the Francophone area with BCRs (Francophone BCR).[66] This common framework is based on the principles provided for in the WP29 working document WP154 on BCRs. Hence, organizations that already have EU BCRs could have their Francophone BCRs approved more easily by French-speaking regulators (and vice versa).[67]

5. **Companies with BCRs Have a Competitive Advantage.** As data protection becomes increasingly important in today's data-driven business world, BCRs can help strengthen customer trust and inspire favorable perceptions of a company. Therefore, by incorporating a comprehensive and effective data protection program, companies with BCRs have a competitive advantage in the global marketplace.

---

[63] CNIL was appointed rapporteur of the WP29.

[64] *See* WP212, Opinion 2/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross-Border Privacy Rules submitted to APEC CBPR Accountability Agents (2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf.

[65] AFAPDP was founded in 2007 and includes around 30 French-speaking DPAs and governments from countries around the world (including non-EU countries) that are members of the International Organization of the Francophone Area (OIF). For more information, *see* AFAPDP's website, *available at* http://www.afapdp.org/.

[66] Resolution adopted during the 7th General Assembly of the Association of French-Speaking Data Protection Authorities, version from February 6, 2014 (Feb. 6, 2014), *available in French at* http://www.afapdp.org/wp-content/uploads/2013/09/RCE-modifi%C3%A9e-2014.pdf.

[67] To date, 13 French-speaking DPAs of the AFAPDP are able to accept Francophone BCRs to frame transfers of personal data outside of their country: Albania, Andorra, Belgium, Benin, Burkina Faso, France, Gabon, Luxemburg, Morocco, Mauritius, Senegal, Switzerland (federal) and Tunisia.