Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 16, NUMBER 3 >>> MARCH 2016

European Union

EU Regulation Binding Corporate Rules Under the GDPR—What Will Change?

By Anna Pateraki

Binding Corporate Rules (BCRs) are a compliance mechanism with growing importance for global data transfers. They are internal corporate rules, such as codes of conduct, that govern intragroup data practices in a binding and consistent manner worldwide. BCRs demonstrate accountability and build data protection and security into a company's DNA. Within the constantly changing landscape of international data transfers (triggered by the Snowden revelations in 2013 and culminated in the invalidation of Safe Harbor on Oct. 6, 2015, followed by the announcement of the draft Privacy Shield in February 2016).[1] BCRs offer a solid and comprehensive solution for global data transfers. With currently 80 companies having BCRs in place, the number of BCRs is expected to continue to increase.[2]

The adoption of the EU General Data Protection Regulation (GDPR) will change the approval process of BCRs, which will involve the "consistency mechanism" and Commission implementing acts. However, the new process will have a number of benefits for

Anna Pateraki is senior associate for Hunton & Williams LLP in Brussels.

[1] *See* press release of the European Commission of Feb. 29, 2016, "European Commission presents EU-U.S. Privacy Shield."

[2] At the time this article was being finalized, 80 companies had BCRs in place, 15 of which were approved within the last 12 months. *See* European Commission, List of companies for which the EU BCR cooperation procedure is closed.

companies and is expected to be streamlined in the future with a view to speeding up the process of BCRs approvals.[3]

I. Update on the GDPR

1. Status of the GDPR

On Dec. 15, 2015, the European Parliament and the Council of the European Union (Council) reached political agreement on the upcoming GDPR (15 WDPR 25, 12/18/15), which is expected to be officially adopted in the first half of 2016. Currently, the text is being finalized from a legal and linguistic perspective by the EU's legal services who perform technical adjustments to the text. While minor changes to the text remain possible until all procedural steps have been finalized, these are not expected to have significant impact on the core elements of the GDPR. Therefore, the version of the text discussed in this article (version of Jan. 28, 2016) is considered to be very close to final.[4]

In terms of next steps, both the Council and the Parliament will need to adopt the GDPR separately. The Council is expected to adopt the GDPR during the next Justice and Home Affairs (LIBE) Council meeting, which will take place on April 21, 2016. After that, the Parliament will have to receive a recommendation from the LIBE Committee and then adopt the GDPR in a plenary vote, expected for May–June 2016. In the same plenary session, the GDPR will be finalized with the signatures of the presidents and secretaries-general of both the Council and the Parliament, followed by publication in the *Official Journal of the European Union* (EU) within a few days from signing. The GDPR will take effect 20 days after publication in the *Official Journal* and will become applicable two years after that date (Article 91).

2. Two-Year Transition Period

The GDPR provides for a two-year transition period until it will apply directly in all EU Member States, thus replacing the various national data protection laws. Companies should use this time to adapt their data practices to the new framework and rethink their compliance model, as the stricter regime of the GDPR is expected to reduce the risk appetite. The transition period will also be useful for data protection authorities (DPAs) who will need to restructure their enforcement and cooperation practices, as well as to secure the necessary resources to be able to exercise the additional powers conferred on them by the GDPR. For example, the Article 29 Working Party has announced that it will start working on the development of the IT systems, human resources and budget for the new tasks of the European Data Protection Board (EDPB) that will be its successor.[5]

During the two-year transition period, BCRs will continue to be subject to the same process used today, pending potential further guidance from the Article 29 Working Party.[6] This includes the review of a company's BCRs by the lead DPA, followed by the review of two subsequent co-reviewer DPAs, the confirmation of the reviewed BCRs by the mutual recognition procedure or cooperation procedure, and finally the issuance of national DPA transfer authorizations, where needed.[7]

II. Explicit Recognition of BCRs Under the GDPR

1. BCRs as Appropriate Safeguards

Currently, BCRs are not enshrined in law but are established through the standard practice of DPAs and the guidance of the Article 29 Working Party. Once the GDPR takes effect, BCRs will be explicitly recognized as a mechanism "adducing appropriate safeguards" to the transfers of personal data outside the EU (Article 42 (2)). Importantly, the explicit recognition of BCRs covers both BCRs for controllers[8] and BCRs for processors[9] (Article 4 (17)). In addition, BCRs will be available not only to a corporate group but also to a "group of enterprises engaged in a joint economic activity" (Recital 85), which may be interpreted to include business partners.

In the context of examining the validity of the draft EU-U.S. Privacy Shield, the Article 29 Working Party has announced it will also examine the validity of data transfers to the U.S. under the BCRs.[10] In any event, potential upcoming statements or updates to the existing BCRs guidance are not expected to impact the essence of the recognition of BCRs under the GDPR.

2. Minimum Content of BCRs Under the GDPR

As under the current regime, BCRs under the GDPR must include a mechanism to make the BCRs legally binding on the relevant group entities, as well as a mechanism to grant enforceable rights to individuals (Article 43 (1)).

The minimum content of Binding Corporate Rules enshrined in the General Data Protection Regulation is lessened compared to the more exhaustive requirements currently tabled in the guidance of the Article 29 Working Party.

In addition, the GDPR provides for a minimum content of a company's BCRs document (Article 43 (2)(a) –

[3] For a detailed analysis of the substance of BCRs and the currently applicable approval process, see "Why Do We Need Binding Corporate Rules—A Look to the Future," BNA Privacy & Security Law Report, March 2, 2015 .

[4] *See* text of the GDPR, version of January 28, 2016, Political Agreement (16 WDPR 02, 2/25/16).

[5] *See* Article 29 Working Party, statement of Article 29 Working Party of Feb. 2, 2016.

[6] *See* Article 29 Working Party, Work Program of Article 29 Working Party 2016-2018 stating that the transfers subgroup will analyze the impact of the GDPR on existing transfer tools and the existing DPA cooperation procedure.

[7] *See* European Commission, current BCR procedure.

[8] *See* Article 29 Working Party, the table of Article 29 Working Party on the elements of BCRs for controllers (WP153).

[9] *See*Article 29 Working Party, the table of Article 29 Working Party on the elements of BCRs for processors (WP195).

[10] *See* press release of Article 29 Working Party, Feb. 3, 2016.

   ISSN 1473-3579

(m)), including: a list of entities bound by the BCRs; a description of the data transfers; the binding nature of the BCRs internally and externally; the general data protection principles by which the group will abide, including regulation of onward transfers; the rights of data subjects; what entity within the EU accepts liability for any breaches of the BCRs; how individuals receive notice about the BCRs; the tasks of the data protection officer; the complaint-handling procedures; how compliance with the BCRs is verified; how changes on BCRs are reported to the DPA; how the BCRs entities cooperate with DPAs; how conflicting legal requirements are reported to the DPA; and what personnel data protection trainings take place.

The minimum content of BCRs enshrined in the GDPR is lessened compared to the more exhaustive requirements currently tabled in the guidance of the Article 29 Working Party. Although the core requirements between those two sources are similar in essence, there are some differences including:

- **Principles**. Under the GDPR, BCRs must contain an obligation for companies to describe how they comply with some additional data protection principles, such as the principle of data minimization, privacy by design and by default, and an obligation to define limited storage periods (Article 43 (2)(d)).

- **Profiling**. Under the GDPR, BCRs will have to explicitly give individuals the right not to be subject to profiling (Article 43 (2)(e)).

- **Choice of court**. Under the GDPR, BCRs should give individuals the right to go to court in their country of residence, for example to claim compensation for breach of the BCRs (Article 43 (2)(e) and Article 75). Companies usually want to negotiate the choice of jurisdiction with their lead DPA, to limit legal proceedings to locations where they have facilities to support litigation. The current regime provides this flexibility and BCRs typically provide that individuals can go to court in the country where the company is headquartered in the EU. However, under the GDPR individuals always will have the right to go to their court of residence (Article 75), which may impact the choice of court negotiations.[11]

- **Audit**. Similar to the current regime, the GDPR provides that the results of the audit should be communicated to the company's data protection officer or other person responsible for monitoring compliance with the BCRs, as well as to the board of the company, and should be available to the competent DPA upon request (Article 43 (2)(i)). However, the BCRs for processors per the Article 29 Working Party currently contain much more detail regarding audits. For example, the audit results of the processor should be made available to the controller or the DPA of the controller upon request, and the controller can request that the processor's subprocessors also be audited.[12]

- **Reporting conflicting legal requirements**. Currently, BCRs for processors include reporting requirements about existing or future legislation applicable to the company that may prevent its fulfilling its obligations under the BCRs.[13] Those reporting requirements should be exercised toward the controller or even the DPA of the controller, which is another point for negotiation with the lead DPA. Fortunately for companies, the GDPR seems to limit this otherwise burdensome reporting obligation to be only to the lead DPA.

It remains to be seen how the interplay between the various sources of BCRs requirements will affect the way companies draft or negotiate their BCRs with DPAs. In practice, a company considering BCRs will need to look into the requirements spelled out in various legal sources: (1) the minimum content of BCRs under the GDPR (Article 43); (2) the more elaborative BCRs guidance of the Article 29 Working Party, including upcoming guidance from the EDPB, which will continue to issue guidance on the Regulation (Article 66 (1)(b)); and (3) other procedural specifications that may be introduced by the European Commission via implementing acts (Article 43 (4)).

III. The BCRs Process Under the GDPR

1. BCRs Approval & the Consistency Mechanism

The most significant procedural change under the GDPR is that the BCRs approval process will trigger the "consistency mechanism" (Article 43 (1) and Article 57). The consistency mechanism is a new concept introduced by the GDPR that enhances and formalizes the cooperation of DPAs through their participation in the EDPB. Today, the European DPAs have developed specific mechanisms to cooperate in the context of approving BCRs (i.e., mutual recognition procedure[14], cooperation procedure[15]).

Under the consistency mechanism, DPA cooperation will include more detailed processes, including deadlines, that typically do not apply today. Although today BCRs follow a unique and very specialized approval process, under the GDPR, BCRs will be approved under the same process as other issues (such as those relating to privacy impact assessments, codes of conduct, certification bodies or contractual clauses for data transfers).

Some of the main elements of the consistency mechanism in the context of BCRs include:

[11] Article 29 Working Party, Explanatory Document of Article 29 Working Party on BCRs for processors (WP204 rev.1), *see* rules on jurisdiction.

[12] *Id.*, *see* rules on audits.

[13] *Id.*, *see* rules on mandatory requirements of national legislation.

[14] "Mutual recognition" is a network of currently 21 DPAs in the European Economic Area (EEA) that have agreed to automatically recognize BCRs in their countries once they have been approved by the lead DPA and the two co-reviewer DPAs.

[15] "Cooperation procedure" is the involvement in the BCR approval process of the other 10 EEA DPAs that do not participate in the mutual recognition procedure, who receive the draft BCR and have one month to review and provide comments.

- **Lead DPA**. Similar to the current regime, under the GDPR a company will have to identify the "competent DPA" to initiate the process (Article 58 (1)). Where the applicant company has more than one establishment in the EU, the competent DPA will be the lead DPA, meaning the DPA of the "main establishment" of the company in the EU (Article 51a). However, the GDPR contains detailed provisions about the identification of the main establishment (Article 4 (13)) and the cooperation with other "concerned" DPAs (Article 54a), which companies would need to have investigated before starting their BCR efforts. For example, if there is disagreement between DPAs about which DPA should act as the lead DPA, the issue may be escalated to the EDPB for a binding decision (Article 58a (b)) following specific processes and timelines, thus adding on complexity.

- **Draft decision of lead DPA**. The lead DPA will have to review a company's BCRs and communicate a draft decision to the EDPB before approving the BCRs.

- **Opinion of the EDPB**. The EDPB will be composed of representatives of the 28 EU DPAs and of the European Data Protection Supervisor. The opinion of the EDPB on BCRs should be adopted by simple majority within eight weeks, which can be extended by another six weeks (Article 58 (3)).

- **Decision of the lead DPA**. Once the EDPB adopts its opinion, the lead DPA can adopt a decision to approve the BCRs by taking "utmost account" of the opinion of the EDPB, although the opinion is not legally binding. The lead DPA has two weeks in which to inform the EDPB whether it intends to follow the opinion of the EDPB (Article 58 (8)).

- **Dispute resolution**. If the lead DPA informs the EDPB that it does not intend to follow the opinion of the EDPB regarding the BCRs (e.g., content of BCRs), then any DPA concerned may trigger the dispute resolution mechanism by which the EDPB adopts a binding decision (Article 58 (9) and Article 58 (1)(d)). The GDPR gives to the EDPB legal personality and makes it a body of the EU especially so it can adopt legally binding decisions (Article 64 (1)), which is not the case under the current regime. The dispute resolution mechanism is subject to specific processes and timelines, but it is not expected to be used significantly in the context of BCRs, since DPAs are expected to leverage their existing experience of cooperation in the context of BCRs, to avoid disagreements.

The consistency mechanism is intended to cover a variety of multijurisdictional issues under the GDPR. However, at this stage, it is difficult to understand how it will work in the context of BCRs, given the numerous procedures and short timeframes. Also, it is unclear if the consistency mechanism would give all 28 EU DPAs the right to comment on a company's BCRs documents or if this can somehow be avoided by improving the process in the implementation phase, to achieve a regime similar to today's mutual recognition procedure. Given those uncertainties, the GDPR should have scoped down which parts of the consistency mechanism would apply to BCRs, instead of making a general reference to the whole consistency section, which seems to unnecessarily add on complexity.

2. Implementing Acts

Implementing acts are acts of the European Commission setting out uniform conditions for the implementation of legally binding legislation in all EU Member States (Article 291 TFEU). The rules and general principles for the adoption of implementing acts are set out in Regulation 182/2011.[16] The Commission implementing acts aim at executing preexisting European legislation and they do not create new law.[17]

It remains to be seen what Binding Corporate Rules issues will be regulated via implementing acts and whether any new processes will be introduced that would differ from existing practices.

Under the GDPR, the European Commission can adopt implementing acts to specify the format and the procedures for the exchange of information between controllers, processors and DPAs in the context of the BCRs approval process (Article 43 (4)). Before adopting such implementing acts on BCRs, the Commission will consult with the EDPB (Article 66 (1)(aa)). Currently, the Commission has no executive powers in the context of BCRs, although it participates in the work of the Article 29 Working Party as secretariat. However, under the GDPR the European Commission could play an important role in determining the logistics and processes of BCRs approvals.

The main elements of adopting Commission implementing acts under Regulation 182/2011 are[18] :

- **Comitology**. Before adopting an implementing act, the European Commission needs to consult with a committee consisting of Member State representatives and chaired by a Commission official (comitology). The process involves the Council and the Parliament, which can exercise scrutiny, however without having veto rights. As the implementation of the law is the responsibility of the Member States, the Commission cannot adopt a legislative act by itself.

- **Examination procedure**. The GDPR specifies that the Commission can adopt legislative acts on BCRs following the examination procedure (Articles 43 (4) and 87 (2)). The examination procedure is a comitol-

[16] Regulation 182/2011.

[17] This is different from the delegated acts mentioned in the GDPR, which are a law-making procedure with veto rights of the European Parliament and/or Council (Article 290 TFEU).

[18] For a detailed analysis of Regulation 182/2011, *see* Paul Craig, "Delegated Acts, Implementing Acts and the New Comitology Regulation," November 2011, Sweet & Maxwell, *European Law Review*, Issue 5, 2011.

   ISSN 1473-3579

ogy process (Article 5 of Regulation 182/2011) according to which the Commission submits a proposal to the committee of Member State representatives and the committee needs to deliver an opinion by qualified majority.[19] Simply put, the act is adopted if the committee delivers a positive opinion. If the committee delivers a negative opinion, the act cannot be adopted and the Commission can either submit an amended proposal or refer to an appeal committee, which can decide whether to accept the proposal.

Depending on the outcome of the various stages, including their respective timelines, it can become complex for the Commission to adopt an implementing act. It remains to be seen what BCRs issues will be regulated via implementing acts and whether any new processes will be introduced that would differ from the existing BCRs practices of DPAs. In any event, companies will have to comply with the requirements of those implementing acts, as noncompliance with the implementing acts adopted under the GDPR is regarded as noncompliance with the GDPR and can trigger enforcement action (Recital 118 of the GDPR).

IV. Benefits of the BCRs Process Under the GDPR

Although the consistency mechanism might sound complicated in its whole, it is not expected that DPAs will make full use of it (e.g., dispute resolution) in the context of BCRs for three reasons: (1) the spirit of the GDPR was to simplify and speed up the BCRs approval process in the first place; (2) the GDPR empowers the Commission to adopt implementing acts that are expected to simplify and facilitate the BCRs format and procedures; and (3) the GDPR empowers the EDPB to advise the Commission on BCRs format and procedures, therefore involving national DPAs already at the genesis of those procedures, which can help eliminate disagreements and create a simpler DPA review process (as today with the mutual recognition procedure).

Therefore, the new BCRs process under the GDPR will have a number of benefits to offer, such as:

- **Dealing with one DPA**. Under the GDPR, a company will need to coordinate with one DPA for its BCRs, compared to the currently applicable system of one lead DPA and two co-reviewer DPAs. Also, under the current regime, companies may need to reach out to the various DPAs that do not participate in the mutual recognition procedure and potentially organize meetings with them to close their BCRs approval process. Under the GDPR, the co-reviewer process will no longer be the case, since the consistency mechanism ensures the opinion of all DPAs (hopefully with some simplification in the review process to be specified at a later stage). Dealing with one DPA is very positive for companies, as they can build relationships and trust with their DPA before starting a BCRs project.

- **Abolition of national DPA authorization for data transfers under BCRs**. Under the current regime, companies having their BCRs approved in all relevant countries (via mutual recognition or cooperation procedure) still need to obtain national DPA authorizations in some countries to allow for the transfer of personal data under the BCRs.[20] Since the GDPR does not contain DPA notification and authorization requirements for data transfers, the national authorizations of BCRs will be abolished, where they exist, thus providing a more flexible mechanism in which approval of BCRs and commencement of transfers under the approved BCRs can be merged to occur at the same time. The GDPR does not contain a sunset clause for BCRs approved under the current regime. Therefore, existing national authorizations for data transfers under BCRs will continue to be valid until amended, replaced or repealed by the relevant DPA (Article 42 (5b)).

- **Procedural flexibility**. The GDPR does not exclusively regulate the BCRs process, but gives leeway to the Commission, upon consultation with the EDPB, to create procedural rules in the future as needed to better facilitate the approval process, therefore providing valuable flexibility for companies, similarly to how it is done today with the opinions of the Article 29 Working Party on BCRs.

- **Harmonization**. Today, DPAs in some EU countries do not recognize BCRs (e.g., Portugal), but the explicit recognition of BCRs will help harmonize those inconsistencies due to the direct applicability of the GDPR in all EU Member States.

V. Conclusion

BCRs are the future of data transfers and will continue to increase in number. Within the constantly changing environment of data transfers, BCRs provide for a pragmatic method of integrating data protection into the DNA of a company and demonstrating accountability. Even if some changes may be introduced to BCRs in light of the general discussion of regulators on data transfers, the GDPR provides a solid ground for a bright future of BCRs due to their explicit recognition. Although the consistency mechanism that will apply to the approval of BCRs currently seems complex, the overall process is expected to be simplified at a later stage by Commission implementing acts and the guidance of the EDPB, to essentially speed up the BCRs approval process for companies.

[19] Article 5, Regulation 182/2011 on the implementing powers of the Commission. Qualified majority in the Council means at least 55 percent of the members of the Council, comprising at least 15 of them and representing Member States comprising at least 65 percent of the population of the EU (Article 16(4) of the Treaty on European Union).

[20] Article 29 Working Party, National filing requirements for controller BCR (BCR-C).