Privacy & Data Security ADVISORY ▪

APRIL 20, 2017

Processor BCRs Under the GDPR: Realizing the Potential

Binding Corporate Rules (BCRs) are an intracompany code of conduct that regulates the principles and rules that apply to the processing and transfer of personal data within a company group, including cross-border. BCRs were established through the standard practice of data protection authorities (DPAs) and the guidance of the Article 29 Working Party (WP29). The upcoming General Data Protection Regulation (GDPR) explicitly recognizes BCRs,[1] both for controllers (BCR-C) and processors (BCR-P). It also extends the scope of application not only to a corporate group but also to a group of enterprises engaged in a joint economic activity,[2] for instance joint ventures.

After WP29 endorsed BCR-C as a useful mechanism for data transfers of complex international structures in 2003, several companies adopted them. Instead of having to justify international transfers on an individual basis, and concluding model contracts with numerous parties, BCRs allow a single set of transfer rules for the entire company group. In today's interconnected world, it is increasingly important to easily transfer data wherever needed, and BCRs offer the flexibility required for such elaborate transfers.

A framework for BCR-Ps was introduced much later, in 2012, and their further inclusion in the GDPR was fiercely debated. In endorsing their inclusion, WP29 praised the merits of BCR-P as an optimal solution for international data transfers. At the same time, WP29 held that BCR-P provides more transparency and accountability requirements beyond those provided in model clauses or other transfer mechanisms (e.g., the current Privacy Shield).

To date, 88 companies have had their BCR procedures concluded, 10 of them pertinent to BCR-Ps. This number is expected to rapidly increase in light of the GDPR and the several benefits associated with BCR-Ps.

Increased Flexibility

BCRs will become more flexible under the GDPR. Under the current regime, countries have to first approve their BCRs in all relevant countries through mutual recognition or a cooperation procedure. They still need to obtain national DPA authorizations in certain countries to allow for the transfer of personal data under the BCRs. These transfer permits only allow specific transfers, and any time a company wants to expand or alter its transfers, a new notification and permitting procedure is required. Making things more complicated, BCRs are not recognized in Portugal as a valid legal basis to transfer personal data outside of the European Economic Area (EEA).

---

[1] Article 47, GDPR

[2] Recital 110, GDPR

The GDPR does not contain DPA notification and authorization requirements for data transfers. National authorizations of BCRs will be abolished, which will significantly reduce the time required to introduce a BCR and will increase flexibility altogether. Because of the direct applicability of the GDPR in all EU member states, any remaining inconsistencies (e.g., Portugal) will be automatically ironed out. As a result, processors will likely increasingly rely on BCR-Ps to justify transfers outside the EEA since they will be able to engage in practically unlimited data transfers within their company groups.

Demonstrate Accountability

Under the GDPR, the data transfer rules are also directly applicable to processors. Processors should, therefore, no longer be dependent on data transfer mechanisms put in place by controllers, but rather have their own tools available to comply with these requirements. Besides, WP29 has indicated that a BCR is an organizational accountability tool that has many merits beyond contractual solutions such as the EC model clauses.

For intragroup transfers, BCR-P not only provides a good basis for transfers but also helps demonstrate broader compliance with the GDPR, for instance the principles of accountability,[3] lawfulness of processing,[4] general processing requirements,[5] and security of processing.[6]

Meet the By-Default and By-Design Requirement and Avoid High Fines

GDPR refers to the requirement of ensuring data protection by design and by default.[7] Therefore, companies should introduce appropriate technical and organizational measures so that all the data protection principles are met. This is a relatively wide concept, and high GDPR fines (up to 4% of a company's global turnover or €20 million, whichever is higher) leave no room for experimentation.

To this end, the GDPR provides that an approved certification mechanism, like a BCR-P, may be used as an element to demonstrate compliance with the by-design and by-default requirements. This tangible uplift in compliance may save companies substantial amounts of money.

Reduce a Company's Operational Cost and Administrative Burden

A BCR-P can also reduce a company's overall operational cost. While a processor, a company may be required to make several cross-border transfers across the globe. If it opts for Model Clauses, for example, the overall cost of the process will be higher, and the administrative burden of dealing with several different schemes particularly heavy. The cost of a BCR is significant in the beginning, yet once in place, less time and money is required for daily company operations.

---

[3]   Article 5, GDPR

[4]   Article 6, GDPR

[5]   Article 28, GDPR

[6]   Article 32, GDPR

[7]   Article 25, GDPR

Enhance Customer Confidence

A BCR is a very detailed code of conduct that exposes a company's policies and procedures to regulators and the public. Once enforced, a BCR signals to customers that the company takes its data protection duties very seriously and that their data is in safe hands. Processors may operate in various sensitive industries (e.g., financial services, telecoms, technology) where reputation is extremely important and may have a significant impact on a company's viability and profitability. BCRs communicate a transparent, robust, and holistic data protection approach.

Future Procedural Flexibility

The GDPR gives leeway to the European Commission, upon consultation with the newly introduced European Data Protection Board (EDPB), to create procedural rules in the future to better facilitate the approval process.[8] Since the European Commission may specify the format and procedures for BCR-Ps, it is likely we will experience model BCR approval procedures, which may streamline the BCR approval process even further.

---

[8]   Art. 47(3), GDPR

If you would like to receive future *Privacy & Data Security Advisories* electronically, please forward your contact information to **privacy.post@alston.com**. Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Data Security Group

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Jan Dhont
+32 2 550 3709
jan.dhont@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Jon Filipek
+32 2 550 3754
jon.filipek@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Dominique R. Shelton
213.576.1170
dominique.shelton@alston.com

Brian Stimson
404.881.4972
brian.stimson@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Daniel G. Taylor
404.881.7567
dan.taylor@alston.com

Jeffrey E. Tsai
650.838.2095
213.576.2608
jeff.tsai@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Michael Zweiback
213.576.1186
michael.zweiback@alston.com

**Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com**

ALSTON & BIRD