UiO : Faculty of Law
University of Oslo

Binding Corporate Rules for Cross-border Data Flows in GDPR Era

Candidate number: 7007

Submission deadline: 15 August 2019

Supervisor: Nancy Liu

Number of words: 17947

Abbreviations

A29WP	Article 29 Data Protection Working Party
APEC	Asia-Pacific Economic Cooperation
BCRs	Binding Corporate Rules
CBPRs	Cross-Border Privacy Rules (CBPR) System
Commission	The European Commission
DPA	Data Protection Authority
DPD	European Union Data Protection Directive
EDPB	The European Data Protection Board
EEA	The European Economic Area
EU	The European Union
GDPR	General Data Protection Regulation
MS	Member States of the EU or the EEA
MNC	Multinational Company
OECD	Organization for Economic Cooperation and Development
SA	Supervisory Authority

Table of contents

1 Introduction

1.1 Background

'Binding Corporate Rules' ('**BCRs**') is not a new concept under EU data protection laws. It was first introduced by Article 29 Data Protection Working Party ('**A29WP**') in 2003 in one of its working documents on transfers of personal data to third countries. After developments in more than a decade, BCRs have been formally confirmed by General Data Protection Regulation ('**GDPR**') as '*personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity*'[1].

Based on such definition, BCRs are the internal data protection policies of multinational companies ('**MNCs**') which do business both within and outside EEA. BCR mechanism plays an important role under EU privacy laws – it has been recognized as one of the appropriate safeguards for transferring personal data by EEA controllers/processors to a third country or an international organisation in the lack of an adequate level of data protection acknowledged by the Commission. Such role is largely attributed to the peculiar advantages of BCRs in cross-border data privacy regulation, as opposed to national legislations.

First, while national laws have difficulties in governing overseas activities due to national sovereignty, the enterprises may utilise corporate governance tools to make its members and employees comply with BCRs, no matter where they are. Second, national laws can only set down general processing principles and rules, which shall be developed tailored to the operation of data controllers and processors for implementation; BCRs are prepared by controllers/processors according to EU laws so as to fit into their corporate structure and business operation[2]. Moreover, from a macro perspective, BCRs contain the data protection principles under EU laws, which shall be respected by the non-EEA group members and employees. In this way, BCRs make the spirits and rationale of EU privacy laws spread to other jurisdictions, and would to some extent contribute to global harmonization of data protection legislations.

In light of these advantages, EU legislators expect that such internal policies serve as a useful tool for transferring personal data globally within the same corporate group, in addition to

[1] Article 4(20).

[2] For detailed discussions on the drivers for corporate privacy policies in data protection area, see Moerel, *Binding Corporate Rules*, 95-99.

contractual solutions[3]. Proponents consider BCRs as an efficient tool for framing international data transfers and even the future of global data flows[4]. Although the number of MNCs with approved BCRs is currently small, it has increased faster recent years than the first decade[5]. However, since the birth of BCRs, there are plenty of complaints or doubts from practical and academic perspectives on the approval, content and implementation of such rules.

First, the process for obtaining approval from the European Commission ('**Commission**') on BCRs has long been regarded as cumbersome, lengthy and costly, even after being reformed under the framework of GDPR[6]. The considerable time, money and human resources investments in the application stage discourage companies from initiating the process.

Second, the minimum content of BCRs required under GDPR is concise compared with the criteria set down by A29WP prior to GDPR. Nonetheless, after A29WP subsequently amended its working documents about the elements and principles required in BCRs (namely, WP267 and WP257), such content requirements are actually more stringent and complicated than before. When A29WP invited public input on WP267 and WP257, some associations commented that several requirements set by A29WP on content of BCRs exceed those under GDPR[7]. It is worthwhile to observe the impact by the current documentation requirements.

Third, concerns are also related to the implementation of BCRs. As one mechanism regulating global personal data transfer, BCRs regulation faces the common difficulties with respect to implementation as other data protection rules do. A Commission report once summarized three phenomena accounting for the then poor state of compliance with EU data protection law, which to some extent still affect implementation today:
- *An under-resourced enforcement effort and supervisory authorities with a wide range of tasks, among which enforcement actions have a rather low priority;*
- *Very patchy compliance by data controllers, no doubt reluctant to undertake changes in their existing practices to comply with what may seem complex and burdensome rules, when the risks of getting caught seem low;*

---

[3] A29WP, WP74, 5-6.

[4] Proust and Bartoli, 'A global solution', 35-39. Also see Olivier Proust, 'Why BCR are the future of global data flows', https://privacylawblog.fieldfisher.com/2017/why-bcr-are-the-future-of-global-data-flows. Accessed 12 August 2019.

[5] According to a list updated on 24 May 2018, the number of companies for which the EU BCR cooperation procedure was closed was 132. The Figure in Annex I reflect the increasing number of BCR groups in recent years.

[6] See, for example, Varde, 'A Burdensome Present and a Dubious Future', 38-41; Pemmelaar, et. al., *Practical considerations*, 8.

[7] See, for example, CIPL, 'Comments on WP256 and WP257'; bitkom, 'Comments on Working Papers 256 and 257 '.

- An apparently low level of knowledge of their rights among data subjects, which may be at the root of the previous phenomenon. [8]

In addition to said common difficulties, BCRs face other difficulties arising out of its peculiar nature. BCRs are internal policies within a corporate group, thus their implementation is largely dependent on the group members' voluntary compliance with such rules. Where the self-regulatory burden conflicts with the commercial interests, and if competent authorities lack sufficient resources to supervise the implementation, the risk of deviation by the members from BCRs could increase. Though data subjects shall be rendered rights to enforce the BCRs, individual enforcement might be hindered by disadvantage factors, such as lack of information and expertise, the opaque and complex internal policies, or the economic cost and difficulties to claim rights against companies in different jurisdicitons, etc. The implementation of BCRs is therefore more challenging than data protection legislations.

1.2 Research Questions, Challenges and Method

In light of the above concerns, this paper intends to observe the strengths and weaknesses of BCR regulation in GDPR era, and come out with some proposals to enhance the uptake and effectiveness of BCRs. The main research question is:

- What are the advantages and disadvantages of the BCR regulation under EU laws, and how to enhance the adoption and effectiveness of BCRs?

In order to address the main research question, it is helpful to first look at the policy rationale behind the whole cross-border data transfer regulation, and the role played by BCRs in such system. Based on such high-level understanding, I will analyse the regulatory developments and limits of BCR regulation respectively from the approval process, content requirement and implementation perspectives. So the main research question will be broken down to the following sub-questions:

- What are the policy rationale for cross-border data transfer regulation, and the role and characteristics of BCRs in such regulation framework?
- How to assess the approval process for BCRs, and is there any means to streamline such process and encourage the uptake of BCRs?
- What are the impacts of the content requirements on BCRs, and how such requirements are transformed by organizations in their BCRs?

[8] EU Commission, *First report on the implementation of the Data Protection Directive (95/46/EC)*, COM (2003) 265 final (15 May 2003), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52003DC0265, 12.

- What are the regulatory developments and limitations on the internal and external binding effects of BCRs?

There are challenges for me to address this question. Since BCRs have been put into practice only for a little more than a decade, and the number of companies adopting such rules is still small, there are relatively limited legal literatures or cases on this topic. On the other hand, BCRs are internal data privacy policies of large organizations, and there is very few disclosure (especially those of negative nature) on the application process or actual implementation of such rules due to confidentiality or other reasons. It is therefore difficult to figure out the real problems with regard to this regulation.

As a result, to answer the research questions, this paper primarily takes the theoretical legal research method, focusing on analyzing the related EU laws, working documents issued by A29WP and EDPB, and other legal literatures. Meanwhile, other research methods will be used where appropriate. Empirical research is adopted to examine the approved BCRs of certain MNCs and to refer to second-hand empirical research materials.

1.3 Structure of the Thesis

This paper has a structure as follows:

As a starting point, section 2 of this paper will briefly outline the role and characteristics of BCRs in the context of cross-border data transfer regulation. Section 3 will analyze the provisions on the approval process for BCRs, and discuss ways to overcome the shortcomings of such process. Section 4 will analyse the minimum content of BCRs required by GDPR and the A29WP, and compare statements in some MNCs' BCRs in order to assess the actual effects of content requirements. Section 5 will look into the implementation mechanisms for BCRs, which will be respectively assessed from internal compliance and external enforcement perspectives. Section 6 will be a conclusion part of this paper.

Unless otherwise indicated in the context, the words and phrases used in this paper (including personal data, data subject, controller, processor, etc.) have the same meanings as defined in GDPR.

2 Brief on BCR Regulation

2.1 Policy Rationale for Cross-border Data Transfer Regulation

2.1.1 Mitigating the Risks on Data Privacy Resulting from Data Flows

With the advancement of technology and popularity of Internet, we are embracing the benefits of cross-border data flows. Generally speaking, individuals could use a huge variety of digital services developed in other countries, gain benefits from online communication, enjoy entertainments or learning online, usually after consenting to personal data transfer; companies benefit from globalization of digital economy, and governments and public authorities benefit from international cooperation in sharing information in various areas; and the society as a whole could benefit from the information exchanged internationally and gain economic and social developments[9].

However, the potential risks arising out of cross-border data flows could not be neglected. For example, the level of data protection might be weakened if personal data is transferred to a regime with no or less stringent privacy laws; even there are privacy laws in such regime, it would be more difficult for data subjects to claim rights abroad; transferred data may be accessed by foreign law enforcement authorities; companies may suffer economic and reputational loss if personal data transferred by them are inappropriately disclosed abroad. In light of those risks, a scholar summarize some motivations behind cross-border data transfer regulations: preventing circumvention of national data protection and privacy laws, guarding against data processing risks in other countries, addressing the difficulties of individual in asserting data protection and privacy rights abroad, and enhancing the confidence of consumers and individuals[10].

Accordingly, the cross-border data regulation under GDPR mainly reflects EU regulators' concerns about the potential privacy risks accompanying data transfer. As stated in Recital(101), when personal data are transferred from EEA to recipients in third countries or to international organisations, the level of protection of natural persons ensured in EEA by this regulation should not be undermined, including onward transfers.

2.1.2 Reducing Obstacles to International Data Flows

[9] Kuner, 'Transborder Data Flows', 102-103.

[10] Kuner, 'Past, Present and Future', 22-24.

Despite of potential risks and the necessity of regulation, inappropriate restrictions on data flows and divergent national rules may constitute obstacles to the benefits of global data flows. Some regional instruments address such concerns and have tried to maintain a balance between protecting personal data and reducing legislative obstacles to cross-border data flows. For example, the *OECD Privacy Guidelines* developed in 1980 has claimed to fulfil two aims: one is privacy protection, and the other is to mitigate the risk brought by the competing national data protection laws to the cross-border data flows and global economy[11].

The EU regulators also appreciate the benefits of data flows. First and foremost, the free movement of personal data within EEA has been made one objective besides the other of privacy protection[12]. With regard to personal data transfer outside of EEA, though such transfer should be subject to conditions laid down under EU laws in light of potential risks, such conditions have been evolving from simple, abstract principles under DPD to a concrete, multi-layer regulatory framework under GDPR.

Under DPD, the principle for personal data transfer to third countries is that the third country in question ensures an adequate level of protection. Derogations from such principle are only allowed in specified situations listed by Article 26(1) or complying with Article 26(2). Article 26(2) simply provides that a MS may authorize data transfer to a third country which does not ensure an adequate level of protection if the controller adduces adequate safeguards, in particular resulting from appropriate contractual clauses, with respect to the protection of the privacy and rights of individuals.

In contrast, Chapter V in GDPR lays down more comprehensive, flexible rules for transfers of personal data to third countries or international organisations. Firstly, a controller or processor may transfer personal data to a third country or international organisation which has been assessed and decided by the Commission to ensure an adequate level of protection (hereinafter 'adequacy decisions')[13]. Secondly, in the absense of an adequacy decision from the Commission, such data transfer may occur only if the controller or processor has provided appropriate safeguards, and enforceable data subject rights and effective legal remedies for data subjects are available[14], and the appropriate safeguards explicitly include various machenisms besides contractual clauses. Lastly, where neither of the above conditions are

[11] OECD, '2006 Report', 6.

[12] Articles 1(3) of GDPR: '*The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data*'.

[13] Article 45.

[14] Article 46.

satisfied, the controller or processor may check if the intended transfer fits into any specific situation specified as derogation under Article 49. If none of the above situations is satisfied, the personal data should not be tranferred to third countries or international organisations. Compared with provisions under DPD, such multi-layer regulatory framework offers more legitimate means for data transfer outside EEA.

In short, the development of EU rules on data transfer demonstrates an attempt of retaining a balance between promoting privacy and personal data protection and facilitating the necessary international data movements. Such consideration is also reflected in the *OECD Privacy Guidelines* and data protection instruments in other jurisdictions. We should take these two policy rationales into account when assessing any cross-border data transfer rules.

2.2 The Role and Characteristics of BCRs Regulation

2.2.1 Geographically-based and Organizationally-based Regulatory Approaches

There are different approaches for regulating cross-border data flows, one distinction is geographically-based approach and organizationally-based approach. The geographically-based approach regulates data transfers based on the assessment of whether a certain level of protection is assured by the legal system of the country of data import and of the compliance in practice. A prominent example is the aforesaid data transfer to third countries based on the adequacy decisions made by the Commisssion. The organizationally-based approach makes the data exporters accountable for taking up necessary measures to ensure the continued protection of personal data which they transfer to importers abroad, therefore it is also referred to as the accountability approach[15]. Examples are elaborated in next paragraph. These two regulatory approaches are usually co-exist in one cross-border data transfer regulatory framework, as demonstrated by the aforesaid multiple-layer mechanisms under GDPR.

The appropriate safeguards prescribed under Article 46 are examples of the organizationally-based regulatory approaches. As stated above, data transfer outside the EEA in the absense of an adequacy decision is possible if the controller or processer has provided appropriate safeguards, and on the conditions that enforceable data subject rights and effective legal remedies for data subjects are available. BCR regulation is one of those appropriate safeguards under article 46(2), and it aims to ensure protection of personal data within a group of enterprises by obliging exporter and importer to introduce necessary protections for the

[15] Kuner, 'Transborder Data Flows', 64-76.

individual. Other appropriate safeguards include legally binding and enforceable instrument between public authorities or bodies, standard data protection clauses adopted or approved by the Commission, approved codes of conduct, and approved certification mechanisms.

Currently there are only 13 countries recognized by the Commission as providing adequate protection under the framework for cross-border data transfer in GDPR[16], therefore, the aforesaid appropriate safeguards plays an important role in faciliating international data transfer outside of EEA. Among these appropriate safeguards, BCRs have their particular characteristics in the scope of application, content, implementation and enforcement mechanisms.

2.2.2 The Characteristics of BCRs Regulation

2.2.2.1 Geographical scope of application

Any personal data transfer outside the EEA based on BCRs of a group of organizations only applies to data transfer between members in such group who are bound by the BCRs; other conditions and safeguards should be met and provided if the non-EEA data importer would like to onward transfer such personal data to another third country. In other words, cross-border data transfer based on BCRs requires that data exporters and data importers have corporate or other kind of close relationship.

EU regulators allow a group of organizations to choose and indicate in its BCRs if they apply to i) all personal data transferred from the EEA within the group OR, ii) all processing of personal data within the group.[17] However, even scenario ii) is indicated, the enforceability of BCRs vis-à-vis such group may legitimately differentiate between data originating in the EEA and subsequently transferred abroad, and other categories of data[18].

Besides, depending on the role of the entity who initiates the data transfer in the group, BCRs could be differentiated as BCRs for controllers ('BCR-C') and BCRs for Processors ('BCR-P'). BCR-C applies to personal data transfer made by controllers established in the EEA to other

[16] These countries are Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework). Adequacy talks are ongoing with South Korea. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Accessed 12 August 2019.

[17] A29WP, WP256, 14.

[18] A29WP, WP74, 8.

made by a processor on behalf of an EEA controller and that are sub-processed within a processor's organisation.

2.2.2.2 Content

Unlike the standard data protection clauses which are determined by the Commission or a DPA[19], BCRs are set up, amended or updated under the responsibility of the private entities themselves while subject to approval from competent DPAs. Article 47(2) of GDPR stipulates the minimum requirements on the content of BCRs, and A29WP further sets down detailed guidance on the elements and principles to be contained in BCRs for controllers and processors separately through Working Documents[20]. These mininum requirements must be satisfied when a group drafts its BCRs in order to get the approval on BCRs.

On the other hand, although the minimum content is regulated by law, the BCRs are still internal rules of certain organization. A MNC can draft its own BCRs take into account of its commercial needs and data processing activities. The legislators leave certain rooms for the enterprises to tailor the content of BCRs. For example, Article 47(2) requires BCRs should specify their legally internal and external binding nature. With regard to the internal binding nature, A29WP sets out a non-exclusive list of mechanisms for the group to adopt, as long as the group could demonstrate how the BCRs are made binding on the group members and the employees to the satisfactory of the competent DPAs[21]. The different legal and cultural backgrounds and various business philosophies and practices of the MNCs may also affect the BCR contents.

2.2.2.3 Stipulated self-regulation

The BCR regulation possesses certain elements of both private and public regulation. As Sheehy summaries, public regulation is promulgated by a public authority, depends on the exercise of public legal powers, utilises public resources, and relies on public executive and judicial authorities for testing compliance and enforcement; in contrast, private regulation is

[19] The Commission has issued two sets of standard contractual clauses for data transfers from data controllers in the EU to data controllers established outside the EU or EEA, and one set of contractual clauses for data transfers from controllers in the EU to processors established outside the EU or EEA. See https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en. Accessed 13 August 2019.

[20] A29WP, WP 256 and WP 257.

[21] For instance, A29WP, WP 256, 5-6.

not produced by or dependent upon public resources, and is not implemented by or dependent upon a public regulatory body.[22]

The following characteristics usually make BCRs confused with private regulation: the uptake of BCRs as one tool for cross-border data transfer is voluntary; as internal data protection policies, the content of BCRs are prepared by and tailored for each MNC; and their implementation is primarily dependent upon the compliance measures taken by MNCs other than public powers.

The BCR regulation should however not be simply categorized into private regulation, as its uptake and implementation are also subject to public regulatory system: its function as legal basis for transferring personal data abroad was legally recognized by EU regulators; the content of BCRs should be approved by the competent SAs; and in particular, it is required to grant rights to data subjects to enforce the BCRs by making claims before the competent SAs or courts. In a word, once the uptake of BCRs is approved, they are binding and enforceable vis-à-vis the MNCs.

Such conflated characteristics of BCRs reflect an attempt of legislators to use 'stipulated self-regulation', which means self-regulation accomplished within an existing general legal framework[23], to achieve regulatory outcomes for transnational personal data flows.

In sum, BCRs are drafted by a multinational group in accordance with statutory legislation and approved by the competent SA, and apply to members and employees of such group. The content of BCRs shall satisfy the minimum requirements, while the EU laws leave certain rooms for the organizations to tailor the BCRs to themselves. The BCR regulation blends certain elements of private and public regulation thus is deemed as a 'stipulated self-regulation'.

GDPR formally recognizes BCRs as one kind of appropriate safeguards in cross-border data flows, and reforms and unifies the procudural and substantive requirements in approving BCRs. Thanks to the direct applicability of GDPR to all MSs, any previously inconsistent or contradictory national laws should be ironed out. All of these reforms aim to make the BCR regulation a more attractive data transfer tool. Next sections will analyze the strengths and weaknesses in the approval process, content requirements and implementation of BCRs in GDPR era.

---

[22] Sheehy, 'Understanding CSR', 106.

[23] Moerel, *Binding Corporate Rules*, 245.

3 Approval Process

3.1 The Current Approval Process

The current approval procedure for BCRs are mainly framed in the following instruments:

- Article 47.1(a), 63, 64 and 65 of GDPR,
- Working Document Setting Forth a Co-Operation Procedure for the approval of BCRs for controllers and processors under the GDPR, WP263 rev.01,
- Recommendation on the Standard Application for Approval of Controller BCRs for the Transfer of Personal Data, WP264, and
- Recommendation on the Standard Application for Approval of Processor BCRs for the Transfer of Personal Data, WP265.

Based on said instruments and other related rules and guidance, the approval procedure could be summarized as below[24]:

(a) The applicant group proposes a SA which should act as a single point of contact with the applicant and manage the review and approval procedure ('**BCR Lead**'). The decision on the BCR Lead would be made after the proposed BCR Lead communicates and consults with all SAs concerned[25].

(b) After receiving the draft BCR documents from the applicant, the BCR Lead shall review and comment such documents with the assistance of one or two SAs as co-reviewer and discuss with the applicant. Following discussions and amendments, a 'consolidated draft' of BCRs will be produced by the applicant and forwarded by the BCR Lead to all SAs concerned for comments. The applicant should address satisfactorily all comments in order to reach a 'final draft' of BCRs.

(c) The BCR Lead should submit its draft decision to the EDPB on the final draft of the BCRs together with all relevant information, and the EDPB will adopt a non-binding opinion on this matter for the BCR Lead's consideration.

(d) If the BCR Lead intends not to follow the EDPB non-binding opinion, the EDPB shall adopt a binding decision as dispute resolution according to Article 65. Where the EDPB adopt a binding decision over dispute, or the BCR Lead accepts the EDPB non-binding

[24] A29WP, WP 263 rev.01.

[25] According to footnote 2 of WP263 rev.01, SAs concerned for BCRs approval procedure are SAs in the countries from where the transfers are to take place as specified by the applicants or, in case of BCR-P, all SAs (since a processor established in a MS may provide services to controllers in several - potentially all - MSs).

opinion, the draft BCRs could be finalized and approved based on said EDPB opinion or decision.

3.2 Regulatory Developments

Some regulatory developments introduced by GDPR may affect the approval process of BCRs, including the following aspects[26].

3.2.1 'One-Stop-Shop' Mechanism

'One-Stop-Shop' is a metaphor for the cooperation mechanism between EU SAs. It enables EU controllers or processors to identify a lead supervisory authority ('**Lead SA**'), and the Lead SA shall be the sole interlocutor of them for the processing carried out by them across the EU[27]. The A29WP has issued guidelines particularly clarifying how to determine which SA is the Lead SA for a given controller[28]. And the Lead SA and the other SAs concerned are required to cooperate with each other in an endeavour to reach consensus according to Article 60.

This mechanism only applies to personal data processing activities carried out by a EU controller or processor which (i) take place in the context of the activities of establishments in more than one MS of such controller or processor if it has establishments in multiple MSs, or (ii) take place in the context of the activities of a single establishment of such controller or processor but substantially affects or is likely to substantially affect data subjects in multiple MSs [29].

The appointment and functions of BCR Lead in reviewing and approving BCRs (as summarized in section 3.1) is a scenario reflecting the one-stop-shop mechanism.

3.2.2 Consistency Mechanism

Under DPD, the DPAs in different MSs might adopt different positions on the same issue, and make the regulated persons face inconsistent nature of decisions. The introduction of

[26] Pemmelaar, et. al., Practical considerations, 8.

[27] Article 56.6.

[28] A29WP, WP244 rev.01.

[29] These two situations are collectively defined as 'cross-border processing' under Article 4(23) of GDPR. Since such 'cross-border' has different meaning (i.e. transfer across EU members) from the meaning of 'cross-border' used in this paper (i.e. transfer outside EU), I will refer to these two situations collectively as 'processing activities across EU' or 'processing activities which may affect multiple MSs' in this paper.

consistency mechanism under GDPR is intended to promote the consistent application of data privacy laws throughout the EDPB as a central authority.

This mechanism generally applies to the cases specified in Article 64.1 (including administrative measures in relation to data protection impact assessment, code of conduct, contractual clauses for data transfer and BCRs, etc.) and Article 64.2 (i.e., any matter of general application or producing effects in multiple MSs). For such cases, the competent SA should submit its draft decision to the EDPB, which is composed of the head of one SA of each MS and of the European Data Protection Supervisor ('**EDPS**'), or their respective representatives. The EDPB shall issue non-binding opinion on such cases, and the SA is required to take utmost account of such opinion of the EDPB, otherwise the EDPB is empowered to adopt a binding decision.

3.2.3 No Additional National Authorization or Notification Requirements

Another significant improvement under GDPR is that it abolishes the additional authorization or notification requirements after the approval of BCRs by competent SA. If the controller or processor has provided appropriate safeguards (including BCRs) according to Article 46, it is allowed to make cross-border data transfer, without seeking specific authorization from or notifying supervisory authorities at national level.

3.3 Impacts on the BCR Approval Process

Given it is less than one year since GDPR was implemented, the actual impact of the reformed process is unclear in practice. Among the above regulatory developments, the abolishment of additional national authorization or notification requirements for BCRs simply reduces the bureaucratic processes for using BCRs. It is relatively easily to conclude that such abolishment is an improvement, which makes the process less complex and avoids inconsistent standard between MSs.

On the other hand, the 'One-Stop-Shop' and consistency mechanisms are introduced under GDPR not only for approving BCRs, but also for other decisions by EU regulators with regard to the personal data processing activities which may affect multiple MSs or to certain specified matters. It makes sense to analyze how they would impact the BCR approval process. As the authorities' actual decision-making process under these mechanisms are not open to public, I primarily analyze them by making comparison with the provisions on BCR approval in DPD era.

3.3.1 Cooperation among SAs

The cooperation between SAs across the EU for approving BCRs had been established and operated for more than a decade before the implementation of GDPR. Earlier in 2005, the A29WP issued guidance on the identification of a leading DPA for a BCRs applicant, and established a co-operation procedure between BCR Lead and DPAs concerned in approving BCRs[30]. And a mutual recognition procedure was further developed for speeding up the approval procedure. For DPAs agreeing to the mutual recognition procedure, once the BCR Lead opined that draft BCRs meet the requirements in the working papers, the other DPAs should accept this opinion as sufficient basis for providing their own national permit or authorisation or positive advice for the BCRs. For DPAs that are not part of mutual recognition network, they had one month to review and provide comments within one month upon receipt of the draft BCRs according to the co-operation procedure[31].

Compared with the co-operation framework between DPAs for approving BCRs prior to GDPR, the present arrangement under one-stop-shop mechanism basically succeeds the previous co-operation procedure, which is quite mature after being developed for more than a decade. Therefore, though the one-stop-shop mechanism is a new concept under GDPR, it imposes no significant change to the co-operation procedure particularly set down by A29WP for approving BCRs.

3.3.2 Consistency supervised by EDPB

The most significant procedural change for approving BCRs is the introduction of the consistency mechanism. Under this mechanism, the EDPB is established as a body of the EU, and could make binding decisions on matters submitted to it. Compared with the previous co-operation procedure before GDPR (under which the approval of BCRs is subject to dispersed decisions by all or several SAs concerned), the involvement of the EDPB could in theory enhance the consistency in approving BCRs through the participation of all SAs in the EDPB.

Having said that, since the consistency mechanism has been put into function for only one year, it remains to be seen how it works in the context of BCRs approval. The SAs and members of the EDPB may need some time to familiarize themselves with the practical operation of such mechanism. Meanwhile, at the initial stage EDPB may face large numbers

[30] A29WP, WP107.

[31] See the fourth step of 'Approval of binding corporate rules' on https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en.

of requests from SAs on the application of GDPR in a short period, which may lead to inconcsistent application of provisions thereunder[32].

On the other hand, this mechanism is designed to generally cover a variety of multijurisdictional issues under the GDPR, thus it is not tailored for approving BCRs. Before a BCR application case is submitted to the EDPB, the draft documents have been circulated, reviewed, discussed and amended among the applicant, the BCR Lead and other SAs concerned, followed by a draft opinion of BCR Lead[33]. After that, according to the general provisions of the consistency mechanism, the EDPB shall issue a non-binding opinion 'by simple majority of the members of the Board'; for cases with disputes, the EDPB shall adopt binding decisions 'by a two-thirds majority of the members of the Board'. Since the representative of each SA is also member of the Board, according to the general rules, all the SAs have voting rights to comment the BCRs documents. It is unclear if there is any mechanism to avoid overlapped or inconsistent comments by one SA concerned on the same case. Even the consistency of comments by each SA concerned could be achieved, such double-review procedure adds on unnecessary complexity in getting BCRs approved.

3.3.3 Efficiency in the Procedure

The cumbersome and lengthy procedures in approving BCRs have been previously complained about most, and discourage plenty of organisations interested in adopting such mechanism for cross-border data transfer. Unfortunately, such problem seems unlikely to be solved in a short run under the GDPR framework.

The consistency mechanism is introduced as a new step in addition to the co-operation procedure, hence it naturally would extend the approval process of BCRs. Firstly, the EDPB members will review the draft BCR documents and opinion from BCR Lead before voting. This means that the BCR Lead and the applicant organisation have to accommodate the comments from representatives of all SAs. Then, in case of disagreement between BCR Lead and the EDPB, a dispute resolution procedure shall follow, which could further delay the BCR authorisation. Though the dispute resulotion mechanism might not be often used in the BCRs approval process thanks to the previous experiences between SAs in cooperation with each other[34], we could not rule out the possibility of further delay.

---

[32] White & Case LLP, GDPR Handbook, Chapter 14.

[33] See Section 3.1.

[34] Pateraki, 'What Will Change'.

To recap, though the consistency mechanism enhances the cooperation between SAs and the consistency in decision-making, it brings potential risk in making the approval process for BCRs more complex and lengthy than before. It is necessary to adopt further implementation acts or guidelines in order to coordinate and simplify the current procedures.

3.4 Recommendations

3.4.1 Differentiate Aim and Focus of Works at Two Phases

As stated above, the current approval process for BCRs comprises two phases: the co-operation procedure among SAs and the consistency mechanism supervised by EDPB.

The co-operation procedure basically succeeds the arrangements prescribed by the A29WP for approving BCRs. At this stage, the BCR Lead, co-reviewer(s) and SAs concerned should have reviewed, commented and perhaps made several rounds of discussions and negotiations with the applicant over the BCR documents, which leads to the 'final draft' BCRs and draft decision by the BCR Lead. Works at this stage shall ensure that the draft BCR documents and accompanying procedure within the applicant group generally aligned to the requirements under EU laws.

The consistency mechanism involves the members from all SAs and EDPS, and is designed to make sure the consistency of SAs' decisions on major matters. Hence EDPB should better focus its attention and limited resources on significant issues, such as disagreements between SAs in the implementation of EU laws, and any deviation by SAs from legal requirements. With regard to the BCRs approval, EDPB should avoid duplicate efforts spent on the regular issues, but focus on some ambiguious GDPR rules in need of unified interpretation.

Take the expansion of BCRs to apply to 'a group of enterprises engaged in a joint economic activity' for example[35]. Due to the lack of definition and criteria on such term, divergence may occur between SAs when they determine the eligible group adopting BCRs. Given the interpretation of such term may affect the effectiveness of BCRs, it should not be interpreted too broadly. Before the Commission or EDPB sets down general criteria for defining such term, it should be EDPB who make decisions over individual cases at the BCR approval stage.

[35] For detailed introduction see sub-section 5.2.2.3.

In short, different purposes and focuses of works should be assigned for the two phases of BCR approval. And given the consistency mechanism is generally prescribed for multiple situations, it should be tailored for BCRs approval.

3.4.2 Tailor the Consistency Mechanism for BCR Approval

To avoid repetitive works with the co-operation procedure, the EDPB should take full advantage of the works already done in the co-operation procedure, and tailor the review and decesion-making procedures in the second phase.

Firstly, the Board is composed of representatives from all SAs, some of the SAs might have joined the cooperation procedures before, and shall vote in the Board for the same case as required under the consistency mechanism. To save time and cost, the Board may consider saving such SAs from carrying out another comprehensive review on the draft BCR documents, if they have agreed or deemed to be in agreement with such documents in the first phase. And, if there is neither significant divergence nor new issues coming out with regard to the applicant and the draft documents, such SAs shall keep their opinions consistent in the two phases of the same case.

Meanwhile, it is not clear whether the mutual recognition procedure joined by most of SAs for approving BCRs is still valid after the implementation of GDPR. If the answer is positive, the EDPB could consider utilising such mutual recognition procedure to coordinate the opinions of Board members too. For instance, if a set of BCR documents are acceptable by a BCR Lead which has joined the mutual recognition procedure, the other SAs which are also part of the mutual recognition procedure shall, in principle, vote for that case in the Board without further review of such documents.

3.4.3 Foster the Interoperable Accountability of BCR Regulation

The above recommendations focus on streamlining the BCR approval process itself. In a broader picture, BCR regulation is only one of the organizationally-based data protection tools within and outside the EEA. At different stages[36] or jurisdictions, organizations may choose different tools which are suitable for their business needs and data processing operations. Those different tools more or less share commonalities in requirements in data protection field. Hence it is possible create interoperability between the BCR regulation and

[36] For instance, the micro, small and medium-sized enterprises ('**SMEs**') may prefer data protection codes of conduct or certification mechanisms, which take account of the specific needs of the SMEs or the specific features of the various processing sectors.

other accountability approaches, and use such interoperability to make the BCR approval process more efficient.

3.4.3.1 Interoperable with other accountability approaches in EEA

Since BCR regulation and other adequate safeguards under GDPR serve for the same data protection principles and rules, it makes sense to leverage their commonalities to simplify the approval process. This paper primarily takes the codes of conduct and certification mechanisms as examples.

Article 40 encourages the associations and other bodies representing categories of controllers or processors to prepare, amend or extend codes of conduct to contribute to the proper application of the GDPR. Meanwhile, Article 42 encourages, particularly at the EU level, the establishment of data protection certification mechanisms and of data protection seals and marks to enhance transparency and demonstrate compliance with the GDPR. Such code of conduct or certification mechanism alone, when approved pursuant to GDPR and accompanied by the binding and enforceable commitments of the controller/processor outside the EU to apply the appropriate safeguards, is recognized as appropriate safeguards for cross-border data transfer. Some organizations already equipped with the approved codes of conduct or certifications may consider adopting BCRs for intra-transfer in the group. It would benefit both the organisations and SAs if such organisations are able to leverage the approved codes of conduct or certification to simplify the BCR approval process.

To create interoperability between BCR regulation and another accountability mechanism, firstly, such other accountability mechanism should also apply across the EU. For example, it could be a code of conduct with regard to the transfer of personal data outside EU[37], or a EU-wide certification, seals or marks on an organisation's internal data privacy program[38]. Then, the competent authorities (preferably under the lead of the Commission or EDPB) may assess the commonalities and differences between the BCR regulation and the other mechanism, and issue a comparison table and guidance. Such guidance could facilitate the organizations to prepare its BCR application based on the approved accountability mechanism. Finally at the BCR approval stage, the SAs could give credit to the common elements which have been approved under the other accountability mechanism, and focus on reviewing the specific criteria of BCR regulation. In this way the BCR approval process may be speeded up.

---

[37] Article 40.2(j).

[38] Accroding to Article 42.1, the object of certification are 'processing operations by controllers and processors'. It is unclear whether an organisation's data privacy program falls into such 'processing operation' which is capable of being certified under GDPR.

Particularly, the interoperability between BCR regulation and EU data protection certification mechanisms would facilitate the BCR approval process by making use of the certification services offered by the certification bodies. GDPR requires certification bodies to be independent and have an appropriate level of expertise in relation to data protection, and such bodies should be accredited and supervised by competent SAs or national accreditation bodies[39]. Therefore, if the data protection measures of any organization have been certified under a certification scheme, and such measures are also required element in BCRs, the SAs concerned could use such certification to assist their review of BCRs to decide whether such organization has provided sufficient safeguards for cross-border data transfer[40].

Besides, the interoperability between BCR regulation and EU data protection certification mechanism could be used for accreditation in reverse direction. As CIPL[41] comments, BCRs are a de facto form of certification of an organization's privacy compliance program and a 'badge of recognition' by SAs. Hence if a common EU GDPR baseline certification could be established in future, the BCR-approved companies may be given credit for their BCRs towards GDPR certification insofar as the BCR regulation meet the relevant certification criteria.[42]

3.4.3.2 Interoperable with accountability approaches in other jurisdictions

As of January 2015, the majority of countries around the world had enacted privacy or data protection laws to tackle the increased risks and threats to personal data[43]. Some regional and international intergovernment organisations have also adopted data protection laws or guidelines. Most of these privacy and data protection instruments across the world originated or learned from the *OECD Privacy Guidelines* of 1980 or the *Council of Europe Data Protection Convention* of 1981 and share some common characteristics[44]. Meanwhile, regulators in different jurisdicitons gradually appreciate the important role played by the accountability of private actors in data privacy laws, and adopt various organizationally-based

[39] Article 43.

[40] WP173, paragraph 68.

[41] CIPL stands for Centre for Information Policy Leadship, which is a global data privacy and cybersecurity think tank in the law firm of Hunton & Williams.

[42] CIPL, 'Certifications, Seals and Marks under the GDPR', 12.

[43] See Global data privacy laws 2015: 109 countries, with European laws now in a minority. Privacy Laws & Business International Report, Issue 133, February 2015.

[44] For an overview of intenraiontal data privacy codes and national data privacy laws, see Bygrave, Data Privacy Law, 33-116.

regulatory approaches to regulate cross-border data flows, such as the BCRs, APEC CBPRs, the U.S.-Swiss Safe Harbor Frameworks and the EU-U.S. Privacy Shield.

As many business organisations carry out data processing globally thus are subject to data privacy laws in different jurisdictions, many global companies are seeking a single set of internal privacy rules to address data privacy laws in multiple jurisdictions and demonstrate their compliance. Therefore, it procures the regulators to work together and help the organisations achieve such purpose. Cooperation between regulators could faciliate the organisations to apply for authorization or certification of their internal privacy rules in multiple jurisdictions, and also speed up the approval process on the basis of double certification. EU regulators have started trying such cooperation years ago.

In February 2014, experts from the A29WP along with their counterparts from the APEC Data Privacy Sub-Group developed a practical tool (the '**Referential**') to map the respective requirements for the BCRs submitted to national DPAs in the EU and the CBPRs submitted to APEC CBPR Accountability Agents. The Referential indicates a common block describing the main elements which are common or similar in BCRs and CBPRs, and additional blocks presenting their main differences and the additional elements specific to BCRs on one hand and to CBPRs on the other hand.[45] Several companies took advantage of the Referential and achieved approvals under both systems.

Take Merck & Co., Inc. for example. It is headquartered in the U.S., and operates as Merck Sharp & Dohme ('**MSD**') outside of the U.S. and Canada. Its global privacy program was certified by U.S. APEC Accountability Agent, TRUSTe, in 2013 as meeting the program requirements for APEC CBPRs. After that, taking the CBPRs certification as a stating point, Merck utilized the Referential to map and align its privacy policies and procedures from the APRC CBPRs requirements to addressing the EU BCRs requirements. In this way, Merck was able to obtain BCR approval at a significatly lower cost than a traditional BCR approval and months ahead of schedule in 2016.[46] Later in the same year, another multinational company Box, Inc. also received EU BCRs approval based on its global data privacy policies and procedures certifited by APEC CBPRs[47]. Hewlett-Packard is a reverse example which achieved the first dual certification from EU BCRs to APEC CBPRs in November 2014[48].

---

[45] A29WP, Opinion 02/2014.

[46] Cooper and Wandall, 'Interoperable Accountability'.

[47] See https://www.businesswire.com/news/home/20160920005361/en/Box-Extends-Global-Cloud-Milestone-BCR-Approval.

[48] See Angelique Carson, 'Hewlett-Packard First To Win Certification for BCRs, CBPRs', https://iapp.org/news/a/hewlett-packard-first-to-win-certification-for-bcrs-cbprs/.

In sum, since GDPR explicitly provides that BCRs should be approved by the competent SAs, it is unrealistic to devise a third-party review system to ease the burden of SAs in approving BCRs, as some practitioner recommended[49]. But it is possible to explore the possibility of creating interoperability between BCR regulation and other data protection accountability mechanisms, and utilise the reliable assessment of the latter to facilitate the BCR approval process.

3.5 Summary

The current procedures for approving BCRs reformed by GDPR do have some bright sides. First, national authorization and notification requirements for BCRs are explicitly abolished, which reduces some bureaucratic burdens for organisations. Second, the cooperation procedure between SAs have been kept as the first stage, hence the fruitfull experiences over years could be taken advantage of. Further, the introduction of the consistency mechanism and the EDPB as a central authority could promote the consistency in decisions made by the BCR Lead for approving BCRs.

Said that, the consistency mechanism is generally added to the BCR approval process by GDPR, introducing a new phase and new parties into the BCRs approval process. Concerns remain over whether it would add delays and complexity to the process. To streamline and speed up the process, the regulators may coordinate the two phases of the approval process, tailor the consistency mechanism and take advantage of the experience of the mutual recognition, in order to advoid repetitive works and inconsistent comments by one SA on the same case.

In the long run, to further simplify the approval process and save time and cost for multinational organizations, the EU regulators may continue looking into the means by which the BCRs approval process is more interoperable with other organizationally-based regulatory approaches within and outside of the EEA.

[49] CIPL, 'Comments on WP256 and WP257', 15.

4 Content Requirements

4.1 Current Rules

As stated, a minimum set of elements required to be stated in the BCRs are set down in Article 47(2). Shortly after the promulgation of GDPR, some practitioners were glad that the documentation requirements for BCRs seemed 'lessened compared to the more exhaustive requirements' [50] tabled in the guidance of A29WP, i.e., the working document WP153. However, they were disappointed when A29WP soon later updates its working documents WP256 rev.01 (hereinafter referred to as '**WP256**' for ease of reference) setting up a table with the elements and principles to be found in the BCRs. The updated document aims to keep its compatibility with the new framework under the GDPR, but it sets down more detailed and concrete requirements. Though WP256 has no legal binding effects, it is indeed a benchmark guidance for all SAs to review and opine the BCRs in practice.

Therefore, this section takes both Article 47(2) and WP256 as point of departure to assess the documentation requirements for BCRs.

4.2 Regulatory Developments

Basically, WP256 retains the structure of criteria in its precedent WP153, which comprise six aspects: binding nature, effectiveness, cooperation duty, description of processing and data flows, mechanisms for reporting and recording changes, and data protection safeguards. GDPR and WP256 develop the documentation requirements for BCRs in the following aspects.

4.2.1 Unified Requirements Apply within EEA

First and foremost, in contrast to DPD, GDPR directly applies to all EEA countries without the need of transposition by national laws, hence ensures consistent regulation in the data protection field. Accordingly, the minimum content of BCRs prescribed under Article 47(2) directly apply to MSs across the EEA.

Meanwhile, the guidance in WP256 is more detailed than WP153, and leaves the SAs and organisations less discretionary power in certain criteria. For instance, in WP153, if it is not

[50] Pateraki, 'What Will Change'.

possible for a group to impose to a specific EU entity to take all the responsibility for any breach of BCRs outside the EU, DPAs might accept other liability mechanisms on a case-by-case basis if sufficient comfort is brought for protecting data subjects rights and enforceability, such as the joint liability mechanism or the liability scheme based on due diligence obligations[51]. While in WP256, if a group is unable to appoint a specific EU entity to take all the responsibility for any breach of BCRs outside the EU, it could only provide that every BCR member exporting data out of the EU on the basis of the BCRs will be liable for any breaches of the BCRs by the non-EU group member which received the data from such EU member.

Another example is the description of the transfers required to be stated in BCRs. According to WP153, some SAs were allowed to require more detailed description of the transfers besides those specified by A29WP[52]; but WP256 directly stipulates more items which the BCRs must contain, and leaves no flexibility to SAs.

4.2.2 Enhanced Protection for Data Subjects

A variety of new provisions with regard to the third-party beneficiary rights for data subjects are required to be incorporated in BCRs. The previous WP153 only generally stated that the BCRs must grant rights to data subjects to enforce the rules as third-party beneficiaries. WP256 further requires that, BCRs should expressly enumerate the minimum rights capable of being enforced by data subjects, and should ensure that the third-party beneficiary clause of BCRs cover those rights, either by making a reference to the clauses/sections/parts of BCRs granting those rights, or by listing all those rights in the third-party beneficiary clause[53].

Meanwhile, data subjects would also benefit from the enhanced transparency requirement. Such enhancement is reflected not only in listing the various information to be provided to data subjects, but also in stipulating the way for providing those information. For instance, Article 12 of GDPR generally requires that the information provided to data subjects should be in a concise, intelligible and easily accessible form, using clear and plain language, and WP256 emphasizes that the delivery of information in BCRs shall be in full, and a summary will not be sufficient[54].

---

[51] WP153, 4.

[52] WP153, 8.

[53] A29WP, WP256, 6-7.

[54] Ibid, 10.

4.2.3 Stricter Obligations on Controllers/Processors

To create an adequate level of data protection, BCRs should be drafted (or amended) to impose more stringent obligations on the entities as required by GDPR than those required in DPD era.

First of all, the BCRs should explicitly state more principles to be observed by the group besides those required in WP153, which comprise the lawfulness of processing, data minimisation and accuracy, limited storage periods, processing of special categories of personal data, and the accountability principle[55].

Besides, the original principles are also strengthened. For example, as regard to security measures, A29WP further requires the group to explicitly incorporate in BCRs a duty to notify any personal data breach to its EU headquarter (or its EU BCR member with delegated data protection responsibilities) and other relevant privacy officer, and to data subjects where the personal data breach is likely to result in a high risk to their rights and freedoms. And any personal data breach should be documented and the documentation should be made available to the SA on request.[56]

Furthermore, the group should commit to adopt new tools prescribed by GDPR to enhance and demonstrate compliance with the data privacy requirements, which are discussed in section 5[57].

To sum up, the more detailed documentation requirements laid down by GDPR and A29WP would make the BCR regulation better serve its functions as cross-border data transfer tool. It unifies the minimum content of BCRs within EEA so as to reduce regulatory barriers to international data flows on one side, and raise the level of data protection for individuals on the other side.

4.3 The Implications of Reinforced Content Requirements

As stated, the content requirement set down by GDPR combined with the relevant guidelines by A29WP is more abundant than those prior to GDPR. Even compared with other contemporary accountability mechanisms (such as APEC CBPR, EU-US privacy shield), such requirement for BCRs seems more comprehensive and stringent in general. For instance, with

[55] Ibid, 16.

[56] Ibid, 16.

[57] See Section 5.2.1.1.

respect to substantive standards, BCRs shall contain the limited storage period principle, privacy by design and default and more individual rights; with respect to the compliance and enforceability, BCRs shall state the internal and external binding nature of BCRs, and adopt mechanisms (such as the allocation of liability to a specified EU entity, burden of proof reversal, etc.) which better facilitate data subjects to enforce the BCRs. [58]

Therefore, this section will not comment on the content requirements themselves, but observe and analyze their impacts on the BCRs adopted prior to GDPR, on the administrative burden of SAs, and how these requirements are addressed by different companies in their BCRs in practice.

4.3.1 Amendments of the BCRs Adopted prior to GDPR

Article 46.5 of GDPR provides that authorisations made by a MS or SA on BCRs in accordance with Article 26.2 of DPD shall remain valid until amended, replaced or repealed, if necessary, by that SA. Said that, A29WP requires that groups with the BCRs approved before GDPR should bring their BCRs in line with GDPR requirements, and notify relevant changes to all group members and to the SAs concerned. No new approval is required for such amendment. [59]

While many MNCs have updated and publicized their BCRs, a few MNCs still have not done so according to publicly available information. For instance, the BCRs of ABN AMRO Group N.V. displayed on its website is dated November 2012[60], and the BCRs of Airbus Group is dated 13 October 2014[61]. Inaction of groups may be contributed to the non-binding nature of WP256, and to the reservation by the SAs of rights to exercise powers under Article 46.5. Transferring personal data outside EEA based on such legally valid but out-of-date BCRs can not ensure the same level of protection provided under GDPR. To implement the enhanced content requirements, SAs have to take some actions, including exercising their powers under Article 46.5, to urge the groups to update their BCRs.

4.3.2 More Challenges and Limited Resources for SAs

[58] For an easy reference of the comparison of the requirements for BCRs with those under other accountability mechanisms, please see figure 1 in Cooper and Wandall, 'Interoperable Accountability'.

[59] A29WP, WP256, 4.

[60] See Annex II.

[61] https://www.airbus.com/content/dam/corporate-topics/corporate-social-responsibility/ethics-and-compliance/Airbus-Binding-Corporate-Rules%20.pdf, accessed 13 August 2019.

4.3.2.1 Increased tasks and responsibilities for SAs

The enhanced content requirement makes the SAs involved in more tasks with respect to the approval, modification and implementation of BCRs.

At the approval stage, along with the expansion of the content in WP256, the BCR Lead and other SAs concerned may take longer time in reviewing and negotiating the draft BCRs with the organizations.

In a process of modifying the BCRs, WP256 requires that any changes to the BCRs or to the list of BCR members should be reported once a year to the relevant SAs, while the counterpart in WP153 requires only any substantial changes to be reported to the DPAs granting the authorizations. WP256 further requires that, where a modification would possibly affect the level of protection offered by the BCRs or significantly affect the BCRs, it must be promptly communicated to the relevant SAs. Such reporting mechanisms also increase the supervisory duties of SAs.[62]

When it goes to the implementation stage, SAs have duties to deal with complaints from data subjects, advise on consultations or communications from BCR entities, supervise BCR entities and carry out data protection audit in specified situations, etc. WP256 requires the BCRs to give more authorities to SAs, which naturally induces more tasks for them. For example, if a data protection impact assessment ('**DPIA**') indicates that a processing would result in a high risk in the absence of measures to mitigate the risk, the company should consult the competent SA; if a law enforcement authority or state security body requests disclosure of personal data and prevents the group from complying with the BCRs, the competent SA should be clearly informed about such request.[63]

Furthermore, the cooperation duties of SAs in the processing activities across EU[64] may occur in each of the above stages, which lead to extra workloads and additional time dealing with such cases.

4.3.2.2 Optimize the allocation of limited regulatory resources

Even in the DPD era, some national DPAs in the MSs were revearled to be unable to carry out the entirety of their tasks because of the limited economic and human resources available to

[62] WP256, 15.

[63] Ibid, 17-18.

[64] Being the one-stop-shop mechanism. See sub-section 3.2.1.

them[65]. Under the GDPR framework, although a majority of the SAs have increased the budget and staff to deal with the increased tasks, they hardly receives the full amount of resources requested[66]. Under such paradox, regulators have to optimize and allocate the limited regulatory resources to the areas which they consider most appropriate.

It is advisable for the SAs to assign more resources to the implementation than the approval of BCRs. First, as analyzed above, the current documentation requirement for BCRs and related guidance are quite matured and detailed. It is therefore a relatively easier task to verify whether the required content has been contained in the BCRs than to evaluate and supervise the implementation of such rules.

Second, the role of SAs in approving BCRs is more substitutable than in implementation of BCRs. By reference to the experience of the accountability approaches in other jurisdictions (for example the APEC CBPRs), it is feasible to engage a third-party certification system to review and certify the BCRs[67]. Then the role of SAs could be shifted from directly approving BCRs to approving the certification bodies and certification criteria to ensure the reliability of such certification system. Unfortunately, currently such third-party certification of BCRs is not possible because of the rules on approval of BCRs and the scope of certificaiton under GDPR[68]. However, as discussed in section 3.4.3.1, to establish the interoperability between BCR regulation and the EU data protection certification mechanisms may be a good start, for fostering a legislative reform in future.

Last, no matter how much comprehensive and protective the content of BCRs is, it is more important to ensure that they are implemented in practice. As stated in Section 1.1, the BCR regulation not only faces the common implementation difficulties as other data privacy rules, but also peculiar difficulties arising out of its nature. Such circumstances make it more urgent for the SAs to allocate more regulatory and administrative resources to supervise the compliance and enforcement of BCRs.

Said that, even the SAs get more sources, they would prefer to '*maximize their resources by intervening mainly in cases where there is a substantial chance of harm to a significant num-*

---

[65] European Union Agency for Fundamental Rights, 'Data Protection in the European Union: the Role of National Data Protection Authorities'(2010), https://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities, accessed 14 August 2019.

[66] EDPB, First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities, February 26, 2019.

[67] CIPL, 'Comments on WP256 and WP257', 15.

[68] See footnote 38.

ber of individuals' in order to warn and encourage other data controllers to comply[69]. Thus in most cases, the pressure for data subjects to enforce BCRs may be a more deterrent factor for the BCR group. And such pressure depends on the quality of the information delivered in BCRs.

4.3.3 The Quality of Information Delivered in BCRs

This sub-section intends to observe how the documentation requirements are put in place in BCRs in practice. For this purpose, I peruse some approved BCRs published online by certain MNCs[70], and compare information provided therein. By such comparison, we could gain some vivid knowledges on the different levels of quality of information delivered by controllers/processors. My empirical study however has several limitations. The BCR examples I selected is only a small fraction of all BCRs approved and can not reflect the average level of all BCRs. Moreover, the BCRs of an organization may comprise a number of documents, some of which are only available internally and to the competent DPAs, or disclosed to related data subjects upon request. So my observation based on public available information may be partial. The analysis therefore does not intend to evaluate the BCRs of any organization, but only to find out better ways to address the content requirements and enhance the quality of BCRs.

4.3.3.1 The comprehensiveness of information

This sub-section takes the different statements on material scope of BCRs as example to observe the comprehensiveness of information. Pursuant to section 4.1 of WP256, the BCRs must specify the data transfers or set of transfers, including the nature and categories of personal data, the type of processing and its purposes, the types of data subjects affected and the identification of the third country or countries. I compare the underlined elements in several BCRs and have some observations below[71].

As to the categories of data transferred, while some companies provide such information simply by defining 'personal data/information' plus some generic examples, Rakuten and First Data Corporation ('**FD**') provide detailed breakdowns of each type of data which may be transferred by them. As to the purposes of processing, Rakuten generally describes it as 'facilitating the provision of services and contract performance, marketing activities, manage-

[69] Kuner, 'Transborder Data Flows', 155.

[70] To make the samples more typical, I select BCRs of organizations in different industries, with different locations of headquarter, and lead authorities.

[71] For the source of BCRs or more information, see Annex II.

ment of suppliers, manage human resources and data analytics', whereas Norsk Hydro and UCB sets down the purpose for each category of data. As to the data subjects affected, ABN AMRO Bank N.V. simply provides that such rules apply to the personal information of its clients and employees, whereas FD and UCB elaborate the scope of each categories of data subjects. Most BCRs imply the third countries to which personal data may be transferred by listing the group members and their jurisdictions of incorporation (including non-EEA members), whereas some MNCs do not provide such information in BCRs but undertake to provide it upon written request to its appointed contacts.

Such review reflects the different levels of comprehensiveness. Some statements offer very basic, general or abstract concept about what the MNCs will do with the personal data; whereas others are more specific, tailored to the business operation of the companies. The latter is absolutely more helpful to raise the awareness of individuals on the data processing activities.

4.3.3.2 The practical maneuverability of information

The maneuverability of compliance with and enforcement information in BCRs differs among organizations. I take the complaints handling procedure in BCRs as one example.

Almost all BCRs I read provide the basic information such as the means by which data subjects could raise complaints, the contact of an internal organ or staffs dealing with complaints, and a timeline for responding to complaints. But some organizations render such process more maneuverability in their BCRs. For instance, article 15 of the BCRs of UCB further sets down the necessary elements of a qualified complaint, the timeline for sending acknowledgment of receipt of complaint to the individual and for sending a substantive response, the procedure and extra timeframe in case of delay of response, etc. Such additional information not only makes the complaint handling procedure more transparent to data subjects, but also facilitates the efficiency of the organizations in solving complaints.

Different level in maneuverability also exists in other aspects, such as audit[72] and other compliance verification procedures. The more practical the BCRs is, the easier for third parties to enforce such rules.

4.3.3.3 The format and manner of information provision

[72] See Annex II.

As mentioned, GDPR and WP256 stipulate that information in BCRs shall be provided in a concise, intelligible and easily accessible form, using clear and plain language. Thus we pay attention to the format and manner of information provision besides the substance.

For the BCRs presented in one single document, the sections and paragraphs are usually well structured, utilising table of contents, serial numbers, indents and different fonts to signal the hierarchical relationship of information. Such format facilitates readers to understand structure and locate information quickly.

Said that, the large volume of BCR content may still discourage individuals to finish reading. Some organizations are more considerate in adopting ways to avoid information fatigue. For instance, MSD uses bold text to highlight the processing purpose, privacy principle, the entity assuming liability for breach by non-EU members[73], etc. Rakuten not only makes all the basic principles bold, but also brings the readers' attention to the key words by underlining them, such as '**Rule 8A - Rakuten will allow individuals to opt out of receiving marketing information**'. Besides, UCB provides one and a half page summary[74] accompanying the 25-page full text of BCRs, so that the data subjects could easily get to know the privacy principles, their rights and ways to exercise such rights.

For BCRs provided in the webpage, organizations could further use a layered approach to present the content, instead of displaying all the information in a single screen. In such case, the design and layout of the first layer should include the most essential information to data subjects, such as the purpose of processing, the rights of data subjects, etc. Such layered approach could help mitigate the tension between completeness and understanding of data privacy rules, by allowing users to navigate directly to the section they wish to read. [75]

4.4 Summary and Recommendations

This section goes through the regulatory developments on the content of BCRs, and analyze the implications they may incur. Specially attention is paid to the different levels of information quality delivered in BCRs.

---

[73] The Global Cross Border Privacy Rules Policy of MSD describes its core commitments supporting compliance with its BCRs. https://www.msdprivacy.com/us/en/cross-border-privacy-policy-rules.html, accessed 14 August 2019.

[74] https://www.ucb.com/_up/ucb_com_home/documents/BCRs%20Summary%20Aug%202018.pdf

[75] For more discussions on the layered approach, see A29WP, WP260 rev.01, page 19-20.

As GDPR only sets down the minimum content for BCRs and grants organizations certain discretion and flexibility in tailoring their own BCRs[76], some MNCs do the minimum necessary to satisfy the EU laws, while others make more efforts to perfect these rules. Thus differences between BCRs in practice are unavoidable. Nonetheless, such flexibility should not be taken as an excuse for reducing the level of transparency provided to data subjects, especially for those information which are essential for data subjects to exercise their rights in BCRs[77]. Then who and how to guarantee the essential information are disclosed to data subjects in a comprehensive, maneuverable and reader-friendly way? The MNCs, regulators and data subjects can make their own contributions in this regard.

First, the MNCs are in the best position to analyze the nature and context of the processing of personal data and the type of data subjects affected, to prioritise the information disclosed, and to decide the appropriate levels of detail and methods for conveying the information. From a legal perspective, the accountability obligation requires controllers to demonstrate the rationale behind their decisions, and justify the level and means of information they provide in BCRs.

Second, at the approval stage of BCRs, SAs could put more weight on the assessment and guidance of the level of transparency disclosed to data subjects therein. Given the increased works of SAs, it could be difficult for SAs to give very detailed drafting advice on every provision in BCRs. To ease such burden, the EDPB can select and publicize some good BCR provisions as model of transparency to guide the BCR drafting and approval.

Further, it could be helpful to involve interested entities (such as the data subjects affected, industry groups, consumer advocacy groups, etc.) to comment the substance and format of BCRs on a case-by-case basis. The MNCs may test the level of comprehensiveness, intelligibility and the modalities of information by way of user testing and seek feedback on how understandable and accessible such information is. Although such process induces more works on controllers, it could assist them to perform accountability obligations by demonstrating the measures they adopt to achieve transparency.[78]

---

[76] See sub-section 2.2.2.2.

[77] As A29WP recommends in WP260 rev.01, such information should include the details of the purposes of processing, a description of the data subject's rights, the processing which has the most impact on the data subject and processing which could surprise them, etc.

[78] A29WP, WP260 rev.01, paragraph 9 and 25.

That being said, no matter how protective and advanced the content of BCRs is, it is more important to deliver compliance to ensure the rules not only exist on paper. Next we turn to discuss the compliance and enforcement of BCRs.

5 Implementation of BCRs

5.1 Introduction

The BCR regulation allows cross-border data flows within a MNC only if the organization commits to adopt the prescribed tools to ensure an adequate level of protection for personal data, which is analogous to a 'Safe Haven' created by such organization according to laws[79]. Effective implementation of BCRs is therefore necessary to avoid any circumvention by organizations of data protection laws through simply adopting but not respecting BCRs. Meanwhile, implementation of BCRs also concerns the credibility of EU data privacy laws. All approved BCRs contain declarations that they are legally binding and enforceable. If they are not respected or difficult to be enforced in reality, doubts on BCRs may arise. Worse still, weak implementation of BCRs may jeopardize the compliance with data privacy rules and even the respect for the whole regulatory system[80]. This section will review and discuss the developments and weaknesses of mechanisms to implement and enforce BCRs.

In an A29WP working document for judging industry self-regulation and its contribution to the level of data protection in a third country, A29WP proposed three functional criteria for judging the effectiveness of protection offered by a self-regulatory code:

- a good level of general compliance
- support and help to individual data subjects
- appropriate redress (including compensation where appropriate)[81].

Though such criteria were set for industry self-regulatory code, they also apply to the assessment of effectiveness of BCRs: the first criterion refers to the level of compliance by group members and individuals with BCRs (namely the internal compliance); the second and third critera address the rights rendered to data subjects for enforcing the BCRs, including institutional support and the remedy available to data subjects when the BCRs have been or are suspected to be breached (namely the external enforcement). We will respectively examine the stipulated mechanisms for realizing the internal compliance and external enforcement of BCRs.

5.2 Internal Binding Effect

[79] Navas, 'Directive on Unfair Commercial Practices', 346.

[80] Reed, *Making Laws for Cyberspace*, 49.

[81] A29WP, WP7, 3-5.

5.2.1 An Overview of Regulatory Developments

The internal binding nature of BCRs requires that MNCs actively take measures to make the group members and their employees compelled to comply with such internal rules. Such internal binding nature is attached greater importance in ensuring the effectiveness of BCRs, since the enforcement of rights of data subjects '*in transfrontier scenarios is always very complex and may involve disproportionate effort for the data subjects*'[82], and the intervention by SAs normally occurs for cases having significant impact.

The internal binding effect of BCRs is realized from two perspectives. First of all, a variety of compliance tools shall be put in place to guarantee a good level of compliance with the BCRs, including:

- an appropriate data protection training programme,
- a network of data protection officers or appropriate staff for monitoring compliance with the rules,
- an audit programme,
- a complaint handling process,
- the accountability principle and related tools.

Meanwhile, in order to make these compliance tools legally binding on every group member and their employees, MNCs are required to adopt approriate mechanisms to provide legal basis for any group members (normally the headquarter) to enforce BCRs against any breach activity.

Next we will first review the regulatory developments on the internal binding mechanisms of BCRs under GDPR framework.

5.2.1.1 Compliance measures

GDPR enhances the compliance mechanisms that BCRs should include to ensure their compatibility with the GDPR data protection standards. Regulatory developments include the following aspects.

First and foremost, BCR-C shall contain the accountability principle, i.e., controllers shall be responsible for and able to demonstrate compliance with the BCRs. BCR-P shall impose a duty for processors to make available to the controller all necessary information to demonstrate compliance. In order to enhance and demonstrate compliance, specific tools are

[82] A29WP, WP74, 10.

required: (i) maintaining a record of all categories of processing activities and making it available to SAs on request, (ii) taking appropriate technical and organisational measures (particularly data protection by design and by default), and (iii) carrying out a DPIA for processing operations which are likely to result in a high risk to the rights and freedoms of natural persons and in other prescribed circumstances.

As to human resource arrangement, BCRs in DPD era are required to include a commitment to appoint appropriate staff with top management support to oversee and ensure compliance with BCRs[83]. Given Article 37-39 of GDPR prescribes the independent role, position and tasks of the data protection officer ('**DPO**') within an organization, the MNCs which designate DPOs[84] shall commit that their DPOs enjoy the highest management support to carry out their tasks, and DPOs shall directly report to the highest management level.

As to other measures to guarantee compliance with BCRs, requirements on data protection training programme, the complaint handling process and data protection audit programme basically remain unchanged, except for some newly added requirements. As to complaint handling, A29WP adds timelimit for MNCs to deal with data subjects' complaints, i.e., one month in principle, which could be extended at maximum by two further months in case of complexity and number of requests[85]. As to audit, A29WP requires the audit result will be communicated to, in addition to the DPO or other privacy officer/function, the relevant board of the controlling undertaking of a group or of a group of enterprises engaged in a joint economic activity[86]. Where approapriate, the result may be communicated to the ultimate parent's board.

To recap, among the above regulatory developments, one salient trend is to strengthen the accountability of organizations to take measures to demonstrate its compliance with BCRs, such as maintaining a record of processing activities, carry out DPIA in specific circumstance, audit plan, etc. Besides, more weight is added to the role played by DPOs and the management layer of MNCs in overseeing the compliance and correcting any deviation.

5.2.1.2 Legally binding mechanisms

[83] A29WP, WP153, 8.

[84] The designation of DPO is only a mandatory requirement for the controllers/processors covered by Article 37.1 of GDPR. However, many BCR groups designate such a position either for compliance with said provision, or out of their corporate governance needs and voluntary willingness.

[85] A29WP, WP256, 11.

[86] Ibid, 12.

Article 47.1(a) of GDPR generally elaborates 'internal binding effect' of BCRs as being 'legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees'. The word 'legally' before 'binding' implies that BCRs should create enforceable obligations which could be upheld in court.

EU regulators set down in WP256 a non-exclusive list of mechanisms for achieving legal binding effect for MNCs to consider[87]. Such list is placed in the 'internally' binding nature section of WP256, but those mechanisms are actually related to the external effect of mechanisms of BCRs[88]. This sub-section focuses on these mechanisms from their internal binding perspective.

Simply put, the means for making BCRs binding on participating entities include intra-group agreement, unilateral undertakings, and other means; and the means for binding on employees include individual and separate agreement(s)/undertaking, clause in employment contract, internal policies, collective agreements, all of which shall be accompanied with applicable sanctions in case of contravention of BCRs, and other means. This paper primarily discusses those mechanisms binding on group entities.

Comparing section 1.2 i) of WP256 (list of mechanisms binding on entities) with the counterpart of its precedent WP153, intra-group agreement and unilateral undertakings remain the major mechanisms suggested by regulators, except for two changes.

First, the adoption of unilateral undertakings is expressly subject to two conditions: (i) the BCR member taking responsibility and liability (hereinafter '**External Responsible Member**'[89]) is located in a Member State that recognizes unilateral undertakings as binding; and (ii) this BCR member is legally able to bind the other members subject to BCRs[90]. The first condition address the long-standing concern that not all MSs recognize the legal binding effect of unilateral undertakings. For example, unilateral declarations or unilateral undertakings do not have a binding effect under the civil law of Italy or Spain[91]. The second condition requires the External Responsible Member to adopt legally enforceable means to bind other group members. These means include requiring all group members directly become signatories to the BCRs, or authorizing the External Responsible Member to sign the

[87] Ibid, 5-6.

[88] Section 5.3.2.1 discusses the external binding effect of such mechanisms.

[89] See section 5.3.1 for more introduction on this term.

[90] A29WP,WP256, 17.

[91] A29WP, WP133, 10, footnote 12.

BCRs on behalf of them, or backing up the BCR with intra-group agreements among group members.

Another change compared with WP153 is the removal of 'internal regulatory measures' and 'policies of the group' from the mechanism list[92]. Though the 'other means' at the end of list allows for other possibilities than intra-group agreement and unilateral undertakings, the removal at least reflects the regulators' doubts on the eligibility of soft internal measures or policies in binding group members.

By the way, the mechanisms binding upon employees basically remain the same. Contractual clauses with sactions binding upon employees are the major mechanisms. The only non-contractual option is 'internal policies with santions'. One possible reason for the retention of such option may be that the employment agreements normally impose an obligation on the employees to comply with internal policies and sanctions for any non-compliance.

5.2.2 Considerations

5.2.2.1 The internal effect of legally binding mechanisms

From the analysis above, we note that both Article 47.1(a) of GDPR and WP256 emphasize the legal effect of mechanisms binding on group members. Regulators set down stricter requirements for the internal enforceability of BCRs, in the hope that the internal enforceability among group members could deter deviations from these rules.

However, even the External Responsible Member is legally able to enforce the BCRs against other members, the possibility for it to actually lodging a claim against another member for remedying any BCR breach is quite remote. First, group members usuallly share close relationship between them, thus could use non-judicial means to order the non-EEA members to take corrective actions. Besides, resorting to judicial authorities may risk publisizing such breach and damage the reputation of a whole group. A more practical function of intra-group agreements may be legal basis for the External Responsible Member to, after it performs liability for paying compensation and remedying breach of BCRs by a non-EEA member, seek redress internally from the latter[93]. Therefore, to enhance the transparency and maneuverability of statements on compliance measures seem a more pragmatic mean to promote internal compliance.

---

[92] We could also see similar removal of mechanisms when comparing Part 2 (Backgroud Paper) of Standard Application for Approval of Binding Corporate Rules in WP264 with the counterpart in WP133.

[93] Moerel, *Binding Corporate Rules*, 132.

5.2.2.2 Enhance the transparency and maneuverability of data protection audit plan

Among all the internal compliance tools, the audit programme is of paramount importance for the BCR group to verify compliance, scan vulerabilities and take corrective actions if necessary. BCRs are required to create a duty for the group to have data protection audits, and describe such audit system therein. WP256 allows room of manoeuvrability to organizations to design their audit programmes, such as who decide the audit programme, who conduct the audit, the coverage and time of audit, and who will receive the audit results, etc.[94]

The aforesaid flexibility may be given by regulators to avoid imposing too much intervention to the corporate governance of MNCs. And in case that the self-reviewing mechanism fails to function well or in situations where SAs deem necessary, the SAs have been authorized by BCRs to conduct a independent data protection audit of any group member. However, without minimum benchmark being laid down, the public statements on audit plan in BCRs vary in specifics and maneuverability[95]. In such case the data protection audit could hardly serve its function in monitoring compliance.

Therefore, more specific audit programme should be provided in BCRs, particularly regarding the requirements on the time of audit and the independence of auditors. WP256 allows the group to take audit regularly or on specific request from the privacy officer. To avoid procrastination and randomness caused by human factors, it is advisable to require BCRs to commit a regular date protection audit programme with a mininum requirement on frequency of such audit, for example once a year[96]. With regard to the auditors, WP256 permits the BCR group to choose internal or external accredited auditors. However, it is sensible for the MNCs to take measures to ensure the independence of internal auditors. For instance, for BCR group with a network of data privacy officers, the audit of compliance by one group member should be conducted by officers of another member. Besides, regulators could require BCRs to list circumstances where external auditors should be engaged, such as there is evidence on the malfunction or corruption of internal audit department, or the operation involves processing a large scale of special categories of data, etc.

---

[94] A29WP, WP256, 12-13.

[95] The table in Annex II contains some statements on audit programme in BCRs publicly available.

[96] Such interval suggestion refers to the certification criteria under APEC CBPRs. Certified organizations thereunder are required to self-verify and attest on an annual basis to the continuing adherence to the CBRP program requirements. See APEC, Accountability Agent APEC Recognition Application, Annex A, 8, p.6.

5.2.2.3 Internal compliance measures for a group of enterprises engaged in a joint economic activity

To enhance the uptake of BCRs, GDPR expands their application from a group of undertakings to also including a group of enterprises engaged in a joint economic activity. According to GDPR, 'a group of undertaking' means a controlling undertaking and its controlled undertakings[97]; and no definition or criterion is assigned to 'a group of enterprises engaged in a joint economic activity' in GDPR or A29WP guidelines. Comapred with the definition of 'a group of undertaking', it is a reasonable interpretation that the controlling relationship is not a necessity in the latter group. That implies BCRs can be used as cross-border data transfer tool by a group of entities from different corporate groups.

In the lack of definition, there are different interpretations on such term in practice. Some scholars suggest adopting a broad application scope, i.e., 'all enterprises that are part of a single franchise system' could constitute such a group[98]; and CIPL believes this term can cover scenarios 'where two groups of companies engage in a formal or commercial and contractual relationship in respect of a provision of a service, development of a product or a joined collaboration or activity which involves some data sharing between two organisations'[99].

However, the structure and relationship between group members have impact upon the internal binding effect of BCRs. A29WP once commented in its first working document regarding BCRs, that BCRs are very unlikely to be a suitable tool for loose conglomerates, since the diversity between their members and the broad scope of the processing activities would make it very difficult to make the BCRs fully complied by all the members[100]. In other words, the compliance level of BCRs is dependent on the commonalities in aims and operations of group members. Thus the internal binding effect of BCRs faces more challenges in binding corporations with diverse management structures to comply with BCRs than in a group of undertakings.

Given GDPR has broadened the scope, it is sensible for the EDPB to first set down criteria for authorizing a group without controlling relationship to adopt BCRs. Among others things, more cautious stardards should be taken when assessing the compliance measures imposed on group members. Basically, each corporation in such group shall incorporate BCRs, including

---

[97] Article 4(19).

[98] Feiler, A Commentary, 71.

[99] CIPL, 'Comments on WP256 and WP257', 14.

[100] A29WP, WP74, 9.

all compliance measures, into its own internal policies and clear all conflicting provisions; and the top decision-making organ of each corporation shall grant authority and power to the board of the group to implement compliance measures and verify such compliance. Second, punitive sanctions like expulsion from such economic group for serious or repeated breaches of BCRs shall be imposed as a practical motivation to urge members to comply with the rules. Further, given the absence of controlling relationship, it is advisable to require all participating members to conclude a legally binding instrument (such as an intra-group agreement) for compliance with BCRs and the remedial and punitive sanctions for any breach. With members from multiple corporate groups, it is more likely for them to take legal actions against other breaching member to motivate the compliance with BCRs.

5.3 External Binding Effect

5.3.1 An Overview of Regulatory Developments

BCRs gain its external binding effect by the enforceability by data subjects and the competent SAs[101]. Compared with the SAs that has full knowledges on BCRs and administrative powers to implement laws, there are more challenges for data subjects to enforce BCRs. So this section focus on the provisions on the enforceability of BCRs by data subjects in GDPR era.

First of all, requirements on the enforceable rights conveyed by the BCRs to data subjects are enhanced in form and substance[102]. WP256 enumerates the minimum rights that should be enforceable by data subjects in detail, and requires all those rights to be expressly covered by the third party beneficiary clause of their BCRs.

Meanwhile, the BCRs must appoint an entity established on the territory of a EEA member ('**External Responsible Member**') to accept responsibility for, and to take the necessary action to remedy any violation of BCRs by non-EEA members, and to pay compensation for damages arising out of that violation. It could be the EEA headquarters or EEA member with delegated data protection responsibilities, or every BCR member exporting data out of the EEA on the basis of BCRs where it is not possible for a group with particular corporate structures to appoint one specific entity to take all the responsibilities for non-EEA members. The External Responsible Member is required to confirm that it has sufficient assets to pay compensation for damages resulting from any breach of BCRs at the application stage for the approval of BCRs.

---

[101] A29WP, WP74, section 3.3.2. In addition, BCR-P could also be enforceable by data controllers.

[102] See section 4.2.2.

Further, more procedural conveniences are provided to data subjects. Previously, individuals covered by BCRs may choose the jurisdiction of the data exporter, the EU headquarters, or the EU member with delegated data protection responsibilities to lodge claims before the court[103]. Now to be compatible with Article 77 and 79 of GDPR, BCRs must confer to data subjects the right to select a dispute resolution location convenient for them. That is to say, a data subject is able to bring their claim before the SA in the MS of his habitual residence, place of work or place of the alleged infringement, or before the competent court where the controller/porcessor has an establishment or where the data subject has his or her habitual residence. The burden of proof rule for damages claimed by any data subject remains the same, i.e., the External Responsible Member should bear the burden of proof to demonstrate that the non-EEA member is not liable for any violation of BCRs and the damages claimed.

5.3.2 Considerations

5.3.2.1 Legal basis creating third party beneficiary rights

Unilateral undertakings and intra-group contracts are two mechanisms listed by A29WP to grant third party beneficiary rights to data subjects to enforce BCRs against any BCR group failing to honour the BCRs. BCRs by themselves, are in principle a unilateral undertaking made by the MNCs. However, because of the differences in civil and administrative law of the MSs, in some MSs, rights could not be granted to third parties by means of unilateral undertakings, like the abovementioned Italy and Spain. In such case, the MNCs have to put in place the necessary contractual arrangements allowing for third-party rights[104].

Although A29WP confirms that in any event intra-group contracts with third party beneficiary rights are legally enforceable across all MSs, and opines the contractual arrangements need not be complex or long[105], organizations naturally prefer unilateral undertakings out of convenience and simplification consideration. After all, using BCRs for intra-group cross-border data transfer originates from the initiative to explore other tools than contracts to deal with international data transfer. In light of such concerns, scholars propose multiple legal grounds for the external binding effect of unilateral undertakings in BCRs. As Moerel

[103] A29WP, WP108, p6.

[104] A29WP, WP74, section 3.3.2.

[105] Ibid.

summarized[106], for the unilateral undertakings which are made public (for instance published on the Internet), non-compliance with these undertakings can be construed under EU law to constitute (i) a violation of the law on misleading advertising[107]; (ii) an unfair commercial practice[108]; or (iii) a violation of the principles of conformity of goods under contracts of sale[109]. For simplification purpose, Moerel suggested the then proposed regulation directly provide BCRs can be enforced as unilateral undertakings by the third-party beneficiaries[110].

Despite of various doubts and suggestions, EU regulators do not provide a *one-size fits all* mechanism in GDPR era. Unilateral undertakings and intra-group contractual arrangements still remain the few options suggested by A26WP to create legal enforceable rights for data subjects. Such position might be attributed to the unwillingness of EU regulators to interfere with the applicable national legislations of MSs on unilateral undertakings [111]. Regarding the proposals to enforce unilateral undertakings in BCRs by invoking the EU consumer protection and competition laws, they are alternative options for data subjects to claim rights, but could not substitute the protection by data protection laws. For one thing, not all data subjects fall

---

[106] Moerel, *Binding Corporate Rules*, 134. As Moerel did in his book, I also insert the relevant provisions of EU law and a brief reasoning in the footnote for each ground for readers' easy reference, but with necessary up-date of the repealed Directive.

[107] Article 2 of Directive 2006/114/EC concerning misleading and comparative advertising [2006] OJ L376/21 provides that, 'advertising' means the making of a representation in any form in connection with a trade, business, craft or profession in order to promote the supply of goods or services, including immovable property, rights and obligations; 'misleading advertising' means any advertising which in any way, including its presentation, deceives or is likely to deceive the persons to whom it is addressed or whom it reaches and which, by reason of its deceptive nature, is likely to affect their economic behaviour or which, for those reasons, injures or is likely to injure a competitor. BCRs for consumers with deceptive nature could qualify as 'misleading advertising'.

[108] See Directive 2005/29/EC on unfair commercial practices, [2005] OJ L149/22, which regulates, *inter alia*, 'any representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers'. Article 6.2(b) provides that 'non-compliance by the trader with commitments contained in codes of conduct by which the trader has undertaken to be bound' is misleading commercial practice, if 'the commitment is not aspirational but is firm and is capable of being verified, and the trader indicates in a commercial practice that he is bound by the code'. Accordingly, if the undertakings in BCRs are referred as privacy statement for the promotion, sale or supply of a product to consumers, any failure to comply with the undertakings may constitute unfair commercial practice. For more detailed analysis on the link between this Directive and BCRs, see Navas, 'Directive on Unfair Commercial Practices', 349-353.

[109] See Directive 1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees, [1999] OJ L171/12. Article 2.2(d) stipulates that the concept of conformity includes conformity with 'any public statements on the specific characteristics of the goods made about them by the seller, the producer or his representative, particularly in advertising or on labelling'. Undertakings in BCRs can constitute such public statements. Unlike the above two Directives, this Directive has a limited scope of application, being the sale of 'tangible movable' consumer goods (Article 1).

[110] Moerel, *Binding Corporate Rules*, 136-137.

[111] A29WP, WP74, 6.

into the definition of 'consumer' under EU laws[112]. They could be employees, suppliers, business partner, etc[113]. Besides, the remedy of non-compliance and redress provided to individuals under comsumer laws and data protection laws are different. For instance, the traditional remedy in unfair competition law is an injunction which generally could only be invoked by consumer associations rather than individuals[114], whereas data subjects has right to receive compesation under BCRs. In light of this, A29WP still requires '*a specific legislative provision on bindingness of unilateral declarations*' if the applicant opts for such mechanism[115].

Given the legal basis for granting third party beneficiary is not harmonized across EU, each group is still responsible to consider the national laws where its External Responsible Member to be located, and choose a legal basis subject to the approval of Lead SA. Sometimes it may be a difficult choice due to the ambiguity of legislations and judicial practice of certain jurisdictions in this regard. Such uncertainty may hinders the effective uptake of BCRs. In the short term, the applicants have to discuss with the relevant SAs concerned in advance before it submits formal application. For the interest of efficience, it may be helpful if the EDPB issues some general and up-to-date guidance on the jurisdictions which expressly accept or deny the binding effect of unilateral undertakings. But in the long run, a pan-European regulatory reform to harmonize the external binding effect of unilateral undertakings may be a final solution to boost the uptake of such instrument.

5.3.2.2 Measures facilitating individuals to enforce BCRs

As the Advocate General Cruz Villalón opined in the Bara case (Case C-201/14), '*the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed, ...and their right to object to the processing of those data,....*'[116]. Such comments apply for data subjects to enforce their rights under BCRs too.

---

[112] According to Directive 2005/29/EC on unfair commercial practices, 'consumer' means any natural person who, in commercial practices covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession.

[113] See some statements on the data subjected affected in the BCR extracts in Annex II.

[114] Moerel, *Binding Corporate Rules*, 134.

[115] A29WP, WP264, footnote 13: '….*in the lack of a specific legislative provision on bindingness of unilateral declarations, only a contract with third party beneficiary clauses between the members of the Group may give proof of bindingness*'.

[116] Judgement of Case C-201/14 of 1 October 2015, Smaranda Bara and Others v Casa Naţională de Asigurări de Sănătate and Others, paragraph 33. http://curia.europa.eu/juris/liste.jsf?num=C-201/14#.

To enhance the awareness by the data subjects of their rights under BCRs seems the most urgent work. According to a study initiated by the Commision in 2008, only 17% of EU citizens were aware of that their personal data can only be transferred outside the EU to countries which ensure an adequate level of protectin for such data[117]. Today more EU citizens are aware of the basic restriction on data transfer outside EU, but BCRs are still strange to average individuals considering the limited number of adopters. The information provided by BCR groups to the public and specifically to data subjects has the greatest impact on their awareness. As analyzed in section 4, to improve the comprehensiveness, practical maneuverability, format and manner of information provision in BCRs can increase transparency to data subjects.

Further, given BCRs are internal rules of MNCs, to enforce them as third-party beneficiaries poses more legal challenges than the enforcement of legislative provisions. Not to mention that MNCs normally own unparallel advantages in resources and expertise compared with a single individual. So the procedural conveniences, such as reverse of proof burden and choice of dispute resolution forum, are helpful to mitigate such disadvantages. The SAs can assist data subjects to claim their rights if the complaints are brought to them. GDPR provides another mechanism beneficial for data subjects to claim rights. Article 80 provides that data subjects shall have the right to mandate '*a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a MS, has statutory objectives which are in the public interest, and is active in data protection field*' to lodge the complaint, to exercie the rights and to receive compensation on their behalf. If any breach of BCRs harms or is likely to harm data subjects on a large scale, collecitve actions may be a userful tools to exercise their rights.

5.4 Summary

To recap, the internal binding effect of BCRs lies in the multiple compliance tools, and the internal legal enforceability of such tools among group members. Given the nature of BCRs and close relationship between group members, organizations naturally prefer ways other than hard-law approaches to tackle breach of BCRs by other members. As such, the compliance tools, especially a data protection audit is a more practical mean to verify compliance and correct deviations. It is advisable for BCRs to specify a regular time for audits, and adopt measures to ensure the independence of auditors. For BCRs adopted by a group of enterprises

[117] Eurobarometer Study (for the European Commission), 'Data Protection in the European Union—Citizens' Perceptions—Analytical Report' (February 2008), <http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf>, p33.

engaged in a joint economic activity, stricter measures shall be taken to ensure internal comliance and enforcement by group members.

Developments on the external binding effect lie in enhancing both the substantive rights and the procedural conveniences of data subjects in their enforcement of BCRs. However, since the legal basis for BCRs to grant third party beneficiary rights to data subjects is still not harmonized within EEA, doubts on the legal binding effect of unilateral declarations may still hindre the effective uptake and enforcement of BCRs. Expect EU regulators to issue some general guidance in this regard, or harmonize the legal basis for the external binding effect of BCRs. Meanwhile, to enhance the awareness by data subjects of BCRs and to provide legal assistance in individual cases may also facilitate them to enforce their rights.

6 Conclusions

Being an organizationally-based regulatory approach, BCRs have its advantages in regulating cross-border flow of personal data, and can contribute to the global harmonization of data protection legislations. The provisions in GDPR on BCRs and related guidelines develop such stipulated self-regulation, but also leaves some defects which may hinder its uptake and implementation in practice.

As to the approval process for BCRs, the introduction of consistency mechanism and removal of national authorization/notification requirement reduce bureaucratic burdens for the applicant, and enhance the consistency in law application. However, the long-standing concern on the cumbersome and lengthy process seems not addressed. This paper recommends perfecting the approval process from the following perspectives. First, the consistence mechanism is newly introduced to regulate a series of multijurisdictional decisions made under GDPR, thus not tailored for approving BCRs. To avoid duplicate works for the co-operation procedure among SAs and consistence mechanism lead by the EDPB, we need to distinguish the aim, focus and task of the two phases of BCR approval process, and leverage the experiences accumulated in the past, such as the mutual recognition procedure among SAs.

Second, the criteria for approving BCRs and other accountability mechanisms (such as the codes of conduct and certification mechanisms) share some commonalities as they all are bound by GDPR principles and rules. The authorities can issue guidelines on the commonalities and differences between BCRs and other accountability mechanisms, which may inspire the organizations approved/certified under other mechanism to adopt BCRs, or vice versa. The authorities could also engage the certification bodies accredited under GDPR to assist in approving BCRs.

In addition, the Referential developed by A29WP and its APEC counterparts to map the requirements for BCRs and APEC CBPRs and the successful dual-certification attempts by some MNCs (e.g. MSD), inspire us to utilize the interoperable accountability between BCRs and similar regulatory approach in non-EEA jurisdictions to speed up the approval process, and to make BCRs more attractive to global companies.

As to the content of BCR, the requirements under GDPR and WP256 are generally more stringent and detailed than those in DPD era. They enhance the protection for data subjects by, *inter alia*, enumerating the minimum enforceable rights, reinforcing the transparency requirements, and require stricter commitments from BCR group. These enhanced requirements induce more works and responsibilities on the SAs as regard to the approval, modifica-

tion and implementation of BCRs. With limited human and financiail resources, the SAs are suggested to allocate more resources to promote the compliance and enforcement of BCRs.

On the other hand, after perusing some approved BCRs publicly available, it is found that the level of comprehensiveness, maneuverability and format of statements in BCRs vary among MNCs, although they are considered to satisfy the minimum content requirements under EU laws. The quality and quantity of information provided in BCRs affect the awareness and capability of data subjects to exercise their rights. To make the essential information delivered in a comprehensive, maneuverable and easily accessible way, the MNCs shall be accoutable for justifying that the substance and format of information in BCRs fit the nature and context of the data processing, and the type of data subjects affected. Meanwhile, the EDPB could select and publicize some good BCR provisions as model of transparency to guide the BCR drafting and approval. Further, it is desirable for the MNCs to seek comment from the interested parties (such as the data subjects affected, industry groups, consumer advocacy groups, etc.) on the substance and format of BCRs on a case-by-case basis.

As to the implementation of BCRs, this paper discusses the internal compliance and external enforceability of BCRs. The internal binding effect of these rules are guaranteed by the requirements on the compliance tools and the legal enforceability of BCRs with the group. As to the latter, regulators set down stricter requirements for the internal enforceability of BCRs, expecting the internal enforceability among group members could deter deviations from these rules. Nonetheless, the possibility for a group member to internally enforcing BCRs against other members for remedy breach of BCRs is quite remote, except for the External Responsible Member to seek redress on compensation internally after it assumes liability caused by a non-EEA member.

Therefore, to enhance the transparency and maneuverability of statements on compliance tools seem a more pragmatic mean to promote internal compliance. In GDPR era, greater importance is attached to the accountability of entities in demonstrating its compliance. A data protection audit is essential in verifying compliance and correct deviations, but the related requirements in BCRs seem too flexible to be compatible with the high-level data protection standards. More specific audit programme should be provided in BCRs, such as the regular interval for audit, measures to ensure the objectiveness of internal auditors, and the circumstances where external auditors shall be engaged.

This paper also concerns about the challenges a group of enterprises engaged in a joint economic activity (i.e. a group without controlling relationship) may face with regard to the internal compliance with BCRs. To bind the group members from multiple corporate groups, more cautious standards are suggested to be imposed on the internal compliance measures.

For instance, to impose punitive sanctions like expulsion from such economic group for serious or repeated breaches of BCRs, and to require the participating enterprises enter into a legally binding instrument (such as an intra-group agreement) for compliance with BCRs and the remedial and punitive sanctions for any breach.

The external binding effect of BCRs primarily lie in the enforceability by data subjects and the competent SAs. This paper focuses on the enforceability by data subjects. GDPR reinforce the substantive rights and procedural conveniences for data subjects to enforce BCRs. But the legal basis for BCRs to grant third party beneficiary rights to data subjects has not been harmonized within EEA, which may hindre the uptake and enforcement of these rules. It may be helpful if the EDPB issues some guidelines on the jurisdictions which expressly accept or deny the binding effect of unilateral undertakings. And a pan-European regulatory reform to harmonize legal basis for the external binding effect of BCRs may be a solution in the long run. Last but not least, to promote transparency of information in BCRs will enhance the awareness of data subjects, and advice and assistance from SAs and even non-profit associations for individual case may facilitate data subjects to enforce their rights in practice.

In short, the BCR regulation conforms to the global trend to utilize organizationally-based approaches in reglating data flows, and its requirements are quite comprehensive and matured throughout the world. Due to the scarcity of related cases and recent empirical literatures, most discussions of this paper are based on theoretical analysis. Along with more MNCs to adopt BCRs and the awareness of individuals of their data privacy, we expect more attentions to be paid to these rules or similar mechanisms, and make them play a greater role in regulating cross-border personal data flows.

Table of reference

Legislations

Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L281

Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L119

A29WP Documents

Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country? adopted by the Working Party on 14 January 1998, WP7

Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, WP74

Guidelines for identifying a controller or processor's lead supervisory authority, WP244 rev.01

Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP256 rev.01

Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP257 rev.01

Guidelines on Transparency under Regulation 2016/679, WP260 rev.01

Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR, WP263 rev.01

Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP264

Recommendation on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP265

Opinion 02/2014 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, Adopted on 27 February 2014, WP212

EDPB Documents

Endorsement of Article 29 Working Party Documents, Endorsement 1/2018, 25 May 2018.

Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, Version 3.0, 4 June 2019.

First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities, February 26, 2019.

Secondary Literatures

Books

Bygrave, Lee A. *Data Privacy Law - An International Perspective*. Oxford: Oxford University Press, 2014.

Feiler, Lukas, Nikolaus Forgó, and Michaela Weigl. *The EU General Data Protection Regulation (GDPR): A Commentary*. Woking, Surrey, United Kingdom: Globe Law and Business, 2018.

Kuner, Christopher. *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press, 2013.

Moerel, Lokke. *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*. Oxford: Oxford University Press, 2012.

Reed, Chris. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012.

Articles

Sheehy, Benedict. 'Understanding CSR: An Empirical Study of Private Regulation'. *Monash University Law Review* 38, no. 2 (2012): 103-127.

Kuner, Christopher. 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future'. *OECD Digital Economy Papers*, No.187, Paris: OECD Publishing (2011). http://dx.doi.org/10.1787/5kg0s2fk315f-en. Accessed 12 August 2019.

Varde, Alejandra. 'Binding Corporate Rules for the Transborder Flow of Personal Information within Corporate Groups: A Burdensome Present and a Dubious Future'. *Norwegian Open Research Archives (NORA)* (2013). http://urn.nb.no/URN:NBN:no-40514. Accessed 13 August 2019.

Pemmelaar,Wanne, Anna van der Leeuw-Veiksha and charlotte Mullarkey. 'BCRs under the GDPR: Practical considerations'. *Privacy Laws & Business United Kingdom Report*. 90 (2017).

Proust, Olivier and Bartoli, Emmanuelle. 'Binding Corporate Rules: a global solution for international data transfers'. *International Data Privacy Law*, 2,1 (2012): 35-39.

Cooper, Daniel and Wandall, Hilary. 'Scaling Data Protection Globally through Interoperable Accountability'. *Datenschutz und Datensicherheit* 41 (2017): 74. https://doi.org/10.1007/s11623-017-0731-1

Pateraki, Anna. 'EU Regulation Binding Corporate Rules Under the GDPR - What Will Change?' *World Data Protection Report* 16(3) (2016).

Rowe, Heather. 'Data transfer to third countries: Transfers of personal data to third countries: the role of binding corporate rules'. *Computer Law and Security Review: The International Journal of Technology and Practice* 19(6) (2003): 490-496.

Navas, Leonardo Cervera. 'The New Directive on Unfair Commercial Practices in the Internal Market as a Promising Tool for the Uptake of Binding Corporate Rules'. *International Review of Law Computers & Technology* 20(3) (2006): 343-359

Other Literatures

OECD. *Report on the Cross-Border Enforcement of Privacy Laws*. OECD/OCDE 2006. http://www.oecd.org/sti/ieconomy/37558845.pdf, accessed 12 August 2019.

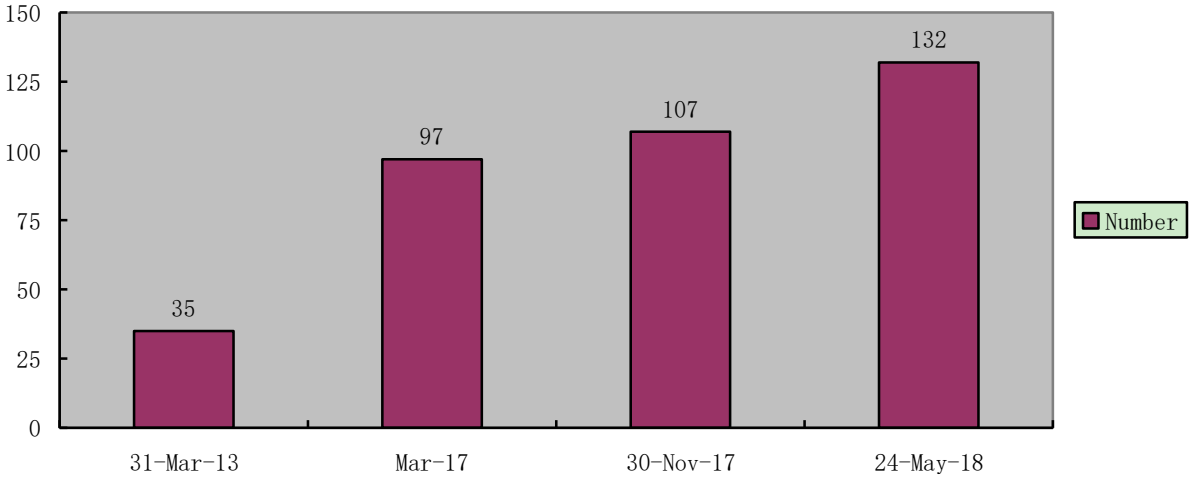
White & Case LLP. *GDPR Handbook: Unlocking the EU General Data Protection Regulation*. https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation, accessed 12 August 2019.

Centre for Information Policy Leadship (CIPL). *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms.*April2017.https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf, accessed 12 August 2019.

Centre for Information Policy Leadship (CIPL). *Comments by the Centre for Information Policy Leadship on the Article 29 Data Protection Working Party's Working Documents Setting Up Tables for Binding Corporate Rules and Processor Binding Corporate Rules adopted on 29 November 2017*. 17 January 2018. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_wp29_bcr_working_documents_wp256_and_wp257_.pdf, accessed 12 August 2019.

Bitkom, 'Comments on Working Papers 256 and 257 on Binding Corporate Rules and Processor Binding Corporate Rules (BCRs)', 18 January 2018, https://www.bitkom.org/Bitkom/Publikationen/Comments-on-Working-Papers-256-and-257-on-Binding-Corporate-Rules-and-Processor-Binding-Corporate-Rules-BCRs.html, accessed 12 August 2019.

Annex I Number of groups for which the BCR cooperation procedure is closed[118]



[118] The figure of 2018 comes from 'BCR overview until 25th May 2018' at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-datah-protection/binding-corporate-rules-bcr_en#listofcompanies, accessed 12 August 2019. Other figures are sourced from the literatures on BCRs, i.e., the figure of 2013 from Varde, 'A Burdensome Present and a Dubious Future', 68-69; the figure of March 2017 from Pemmelaar, et. al., *Practical considerations*, footnote 1; the figure of November 2017 from CIPL, 'Comments on WP256 and WP257', footnote 5.

Annex II Comparison Table for Statements contained in some BCRs

Note:

1. This table only compares several aspects of selected BCRs. For all BCR provisions or more detailed information, check the hyperlinks below. All hyperlinks are accessed on 13 August 2019.
2. Below summaries or extracts come from the BCRs or BCR-related information publicized on the official website of relevant companies, therefore they can not reflect policies made available to competent DPAs and/or related data subjects only.
3. I have perused other BCRs than those listed below for writing this paper. Below table is summarized to support related discussions in the paper.

Items Group(LeadSA)	Norsk Hydro (Norwegian DPA)	First Data (ICO (UK))	Rakuten (Luxemburg DPA)	UCB S.A. (Belgian DPA)	ABN AMRO (Dutch DPA)
Source of Information	https://www.hydro.com/en/privacy/hydros-binding-corporate-rules-bcr/ Public version of Hydro's BCRs, (being extracts the non-confidential information).	https://www.firstdata.com/downloads/pdf/First_Data_Controller_Binding_Corporate_Rules_May_2018.pdf First Data Corporation Controller Data Protection Standards	https://corp.rakuten.co.jp/privacy/en/bcr.html Binding Corporate Rules Policy	https://www.ucb.com/UCB_BCRs.pdf Binding Corporate Rules for Data Protection and Privacy	https://www.abnamro.nl/en/personal/overabnamro/privacy/binding-corporate-rules.html ABN AMRO Group N.V. Binding Corporate Rules
Nature and categories of personal data covered by BCRs	The BCR apply to all personal data, within the Hydro Group, which are protected by applicable EU data protection law. Categories of data include: HR management data, IT-administration data, HSE data, Video surveillance/access logs, Business relations data, Complaints, Investigation information.	Section 19 lists the type of personal data include employment data, customer data, other personal data, anonymised/aggregated data, with detailed elaboration on each type of data. Section 13 indicates the special categories of personal data are also covered.	Personal data processed under the BCRs covers past, present and prospective Rakuten employees, customers, merchants, contractors and suppliers. Meanwhlie, it provides very detailed, non-exclusive enumeration of categories of personal data processed for each type of data subject.	Appendix 2 non-exclusively provides for four general categories of personal data processed/transferred between BCR entities, and details many subtypes on each catogery of data.	Article 1 provides that the BCRs cover the personal information of both clients and employees.

Type and purpose of data processing	Section 3.2 provides an overview of categories of personal data and the purposes for processing each catetory of data.	Section 16 provides a long and non-exclusive list of 26 business purposes for data processing.	Rakuten transfers personal data for the following purposes such as facilitating the provision of services and contract performance, marketing activities, management of suppliers, manage human resources and data analytics.	Appendix 2 non-exclusively provides nine purposes for processing and intra-group transfers.	Article 4.1 sets out the purposes for processing personal data of clients and employees respectively.
Type of data subjects affected	Employees, customers, suppliers and other business partners.	Section 13 provides a non-exclusive list: 1. Our clients and their customers in connection with the provision of services; 2. Individuals initiating payment transactions, including holders of payment instruments; 3. Merchants accepting payments; 4. Employment Data (with detailed breakdown); 5. Other persons as appropriate to conduct its business such as suppliers, partners, contractors and contingent workers and prospective clients of First Data and, in each case, their personnel, external advisors and agents.	Past, present and prospective Rakuten employees (including individual subcontractors, secondees, interns work, experience students, agents temporary and casual workers and their family members/emergency contacts), customers, merchants, merchants' personnel, merchants' end users, contractors and suppliers (including supplier personnel).	Section 3 provides for data subjects covered by BCRs, including patients and caregivers, UCB employees, external workers, healthcare professionals, external vendors.	No specific article addressing data subjects affected. The difinitions on 'Client' and 'Employee' (article 2.3 and 2.6) may help readers understand the scope of this two categories of data subjects.

Identification of the third countries	Section 3.1 provides that the Head of Data Privacy maintains a list of all legal entities to which BCRs applies, with information on their geographical location in and outside EEA.	Controller Schedule 2 provides a list of affiliates that have signed an agreement (i.e. Intra-Group Agreement) and their jurisdiction of incorporation in and outside EEA.	A list of Rakuten Group Entities Part of the BCR Intra-group Agreement publicized at the website indicates the jurisdictions of BCR entities in and outside EEA.	Appendix 1 lists all BCR entities and their jurisdiction of incorporation in and outside EEA.	No specific disclosure in this document.
Audit plan	Section 5.6 provides that Hydro will carry out audits and reviews regarding Hydro's compliance with BCRs.	Section 32 sub-section 10.2: First Data shall conduct regular internal privacy assessments as part of its comprehensive audit programme. Items identified are assigned to **a member of First Data Personnel** who is responsible for developing and executing a remediation plan and associated time frame. Upon completion, the **audit team** will review to determine if the item has been adequately addressed and can be closed or requires additional action and will provide their recommendation to **the Data Protection Officer and to the Board of Directors of the relevant First Data entity** and, where deemed appropriate by the Data Protection Officer, **First Data Corporation**.	Appendix 3 sets out the audit protocol under BCRs, which prescribes the staff and responsibilities of Internal Audit Department, time and scope of audits, auditors, findings report, etc. Among other requirements, audits of BCRs will take place annually in accordance with Rakuten's audit procedure/s; and more frequently at the request of the Global Privacy Manager; and if determined necessary by the Global Privacy Manager.	Section 12 provides for the audit programme. Among others, it provides that the Global Internal Audit Department of UCB shall evaluate and report to the Audit Committee and the Board of Directors, in coordination with the DPO, on applicable aspects of UCB's compliance with the BCRs on a periodic basis or whenever specifically requested by the DPO and as approved by the Audit Committee. Audits of compliance with the BCRs may be undertaken by external auditors, if UCB so decides.	Article 17.2 provides that, audit of ABN AMRO Group will regularly audit ABN AMRO Group systems that Process Personal Data on compliance with this Policy. Audit will plan audit activities with regard to the compliance of this Policy every year.

Existence of intra-group agreement	Information not provided.	Controller Schedule 2 implies there are intra-group agreement.	A list of Rakuten Group Entities Part of the BCR Intra-group Agreement publicized at the website indicates the existence of contractual arrangements.	Information not provided.	Information not provided.