Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CIPL response to the EDPB Draft Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)

Centre for Information Policy Leadership (CIPL)

10 January 2023

The Centre for Information Policy Leadership[1] (CIPL) welcomes the opportunity to comment on the European Data Protection Board's (EDPB) draft Recommendations on the application for approval and on the elements and principles to be found in Controller Binding Corporate Rules (BCR-C) (Recommendations). We understand the goal of the draft Recommendations is to update the existing BCR-C referential in accordance with the GDPR and bring the existing guidelines in line with the requirements set out by the CJEU in Schrems II.

CIPL welcomes the EDPB's efforts to clarify and support the use and further adoption of BCR-C. However, some of the proposed requirements in the Recommendations may instead cause undue burdens to organisations and individuals alike without impacting the level of data protection. In addition to the feedback below, this submission includes an Annex with detailed comments in response to requirements in the EPBD's draft Recommendations.

In particular, CIPL would like to raise the following concerns:

I. ASSESSING THE LEGISLATION AND PRACTICES OF THE THIRD COUNTRY BEFORE ANY TRANSFER

The CJEU's Schrems II ruling has placed additional requirements on parties undertaking international transfers of personal data. The Recommendations require a BCR-C holder to carry out a transfer risk assessment "before any transfer of personal data" from the EEA to outside the EEA takes place. Additionally, the data exporter within the BCR-C group must regularly review risk assessments to determine that the laws and practices in the third country of the data importer do not prevent it from fulfilling its obligations under the BCR-C.

A. Allow BCR-C holders to consider the specific circumstances of data transfers

In line with Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[2] (Recommendations 01/2020), Section 4 of the Recommendations requires a data exporter to implement supplementary measures when necessary to comply with the importer and exporter's commitments under the GDPR. Where the data exporter is not able to implement supplementary measures, personal data cannot be lawfully transferred to a third country under the BCR-C. The section applies the same logic to changes in legislation.

However, Section 4 appears to be taking a strict approach without considering the *specific* circumstances of the transfer or previous experience in the respective country, as is the case with

[1] CIPL is a global privacy and data policy think and do tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Recommendations 01/2020), available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

Standard Contractual Clauses (SCC), for instance.[3] By seemingly creating a higher threshold for transfer risk assessments under the BCR-C than the SCCs, the EDPB risks, in fact, penalizing an organisation that has demonstrated a higher level of compliance and disincentivising organisations from applying for BCR going forward.

Section 5.4.1 of Annex 2 of the Recommendations specifically cites Recommendations 01/2020, which clarify that the exporter will "…need to look into the characteristics of each [transfer] and determine whether the domestic legal order and/or practices in force of the country to which data is transferred (or onward transferred) affect [the transfer]".[4] Furthermore, the same paragraph in Recommendations 01/2020 states, "The scope of your assessment is thus limited to the legislation and practices relevant to the protection of the specific data you transfer, in contrast with the general and wide encompassing adequacy assessments the European Commission carries out in accordance with Article 45 GDPR".[5] In addition, paragraph 33 of Recommendations 01/2020 further acknowledges the need to consider the specific circumstances of the data transfer when assessing the impact of the third country's law and practices and provides a series of elements for the assessment. This analysis is seemingly missing in the EDPB's Recommendations for BCR-C holders and potential applicants.

Similarly, Recommendations 1/2020 allow, when "uncertainties surrounding the potential application of problematic legislation" apply to a transfer, an organisation to proceed with the transfer sans supplementary measures if the organisation finds that it has no reason to believe that the relevant and problematic legislation will be specifically applied to the transferred data and/or importer.[6]

Omitting similar references to the specific transfers in the Recommendations seems in contradiction not only with other Article 46 approved mechanisms but with the EDPB's guidance itself. **CIPL recommends that the EDPB explicitly allow a BCR-C data exporter to consider at least the same elements of a transfer specific risk assessment as provided under Sections 33 and 43.3 of**

---

[3] The SCCs acknowledge under footnote 12 of clause 14 (Local laws and practices affecting compliance with the Clauses) that, when assessing the different limitations and safeguards provided under the recipient country laws, the exporter should account for the specific circumstances of the transfer:

> "As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative timeframe. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies."

European Commission standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN.

[4] Recommendations 01/2020, paragraph 32.

[5] Id.

[6] Id., paragraph 43.3.

Recommendations 01/2020 and under Footnote 12, Clause 14 of the SCCs. Not doing so risks disincentivising the use of BCR in general and penalising certified companies that have a demonstrated commitment to data protection.

B. Onward transfers of data in this context

As mentioned above, the SCCs currently provide a more risk-based approach to data transfers than what the EDPB is seemingly recommending for BCR-C holders. As onward transfers from within a BCR-C, for instance, to service providers will often be based on an SCC, the disparity of approaches between the BCR-C commitments and the SCCs will create a conflict that BCR organisations will not be able to resolve**. The EDPB should allow a BCR-C holder to demonstrate that the likelihood of a third country's government accessing personal data transferred on the basis of additional safeguards is minimal, regardless of the general level of access the government's authorities might have under the relevant legal framework to access that data**.[7]

C. The need for a risk-based approach for intra-group data transfers

Finally**, it is important for the EDPB to adopt a risk-based and contextual approach to the type of data transfers covered by the BCR-C.** These are data transfers within and between different entities of a BCR-C group, in which all entities are under a single control and management structure and bound by the same centrally applied and approved policies and procedures. For this reason, the risk of data mishandling and misuse is generally lower for intragroup data transfers within the same corporate group than in the case of a data transfer to another controller that has its own decision-making power over the data and is subject to its own set of corporate policies and procedures. The data controller in a corporate group will be bound by the same rules and requirements for data processing, including with respect to any governmental access requests, as the data exporter. The EDPB Recommendations should acknowledge this and **apply a risk-based approach to intra-group data transfers.**

II. CENTRALISED ACCOUNTABILITY AND PRIVACY MANAGEMENT PROGRAM

In Section 5.3 of Annex 2 in the Recommendations, the EDPB places various accountability requirements on BCR members. CIPL acknowledges that each entity of a corporate group acting as data importer must comply with the BCR requirements in accordance with the GDPR. However, we have noticed a trend in corporate groups where many of the data privacy program controls and activities, such as the management of records of processing activities and data protection impact assessments, are centralised. Where this model is used, groups demonstrate global compliance at the highest management level and throughout appropriate reporting and management structures.

CIPL suggests that the EDPB revise Section 5.3 of Annex 2 to include the term "BCR-C Group" instead of "BCR members". This will clarify that the BCR group, and where appropriate, in collaboration with

[7] The Administrative Court of Neustadt an der Weinstraße in Germany took a similar position when it held that 2022 census data was not processed in violation of Schrems II despite the integration of a US-based web security service, Cloudflare. The Court cited a public report by Germany's Federal Commissioner for Data Protection and Freedom of Information, in which the Commissioner verified that there was no risk to personal data entered into the census questionnaire. The Court, therefore, ruled that allegations alleging access by U.S. security authorities were speculative under the circumstances and did not stand in the way of data collection. Judgment of 27 October 2022, 3 L 763/22.NW, paras. 65-68, https://www.landesrecht.rlp.de/bsrp/document/MWRE220007662

BCR members, may consolidate the accountability requirements without the need for each member to demonstrate compliance with the BCR-C. Managing records of processing activities, data protection impact assessments and data transfer risk assessments under the BCR-C, including documenting the supplementary measures, as required by section 5.4.1 (iii), can be centralised accordingly.

Finally, CIPL suggests clarifying that the group may designate a single method for submitting individual complaints (for instance, a ticketing system) as prescribed by Section 3.2 of Annex 2. CIPL cautions the EDPB against creating a de facto incentive that individuals can lodge complaints through any available channel, potentially including non-data protection-related resources. This raises uncertainty for the Group when managing individual requests outside of those methods designated for submitting data protection complaints, and CIPL suggests removing this reference in Section 3.2.

III. TRANSPARENCY OBLIGATIONS (INCLUDING ABOUT ANY UPDATES OR SIGNIFICANT CHANGES TO APPROVED BCRS)

The continuous transparency obligations for BCR-C Groups in Section 1.3.1 include the obligation to inform data subjects about any updates to the BCR-C and of the list of BCR members. This requirement is not sufficiently clear because BCR-C holders may regularly update the BCR-C in ways that do not impact individuals. CIPL suggests clarifying this obligation under Section 1.3.1 of Annex 2.

A corporate group with an approved BCR-C should be required to notify individuals only when there is a substantive or material change to the BCR-C that is relevant to individuals, as it affects their rights or position. For example, a change as to how individuals can exercise their rights in relation to the BCR-C. On the other hand, examples of changes which are *not* considered to be substantive or material to an individual include reformatting of the BCR-C documentation and corrections of misspellings and stylistic/ grammatical flaws. Equally, changes to internal controls and procedures that implement BCR-C but do not affect individuals should not be included in the Section 1.3.1 transparency obligation. For example, changes to the process for maintaining records of processing, developing data protection impact assessments, DPO governance and new data privacy roles implementing BCR. None of these are relevant to individuals and their rights, and individuals should not be burdened by this unnecessary information.

The relevant transparency information for individuals is normally included in the version of the BCR-C that is publicly available on the corporate group's website (or on the internal intranet when data subjects are only employees of the Group). CIPL suggests amending Section 1.3.1. to allow the Group more flexibility to communicate the substantive or material changes in the published version of the BCR in such a way that enables individuals to identify said changes. This change to Section 1.3.1 will help reduce compliance costs for BCR-C holders and will avoid confusion for individuals regarding changes to the Group's other existing privacy statements, notices and policies.

IV. FURTHER BCR POLICY CONSIDERATIONS

From a policy and practical compliance perspective, **CIPL strongly believes that the EDPB and European supervisory authorities should proactively promote the wide adoption of BCR and make it easier and more attractive for corporate groups to obtain BCR approval.** Organisations (both controllers and processors) and their senior leadership view BCR as more than just a transfer mechanism. Indeed, BCR demonstrate an organisation's commitment to data privacy. BCR often represent a comprehensive data privacy management program that the corporate group implements consistently across all of its operations and corporate entities globally. The EDPB should use the

"market forces" and further promote and enable the use of BCR, as they ultimately deliver more effective data protection compliance and protection for individuals. CIPL encourages the EDPB to be more explicit in this regard in the Recommendations and also in its future work. In particular, CIPL recommends that the EDPB focus its work on the following points:

a) **It is essential that the EDPB continue working on streamlining the policies and procedures required as part of the BCR application, as well as the approval process itself.** Currently, the requirements and the approval procedures are far too burdensome and lengthy, resulting in a considerable increase in the cost of implementation of the BCR-C. This acts as a barrier for many organisations, who would have otherwise embarked on the BCR route, and favours those that chose alternative transfer mechanisms. Importantly, corporate groups should not face additional hurdles to choosing BCRs as a main mechanism for international data transfers (beyond the initial investment in the BCR implementation and approval process).

b) **There should be mutual recognition of BCR holders between the DPAs in the EU and the UK ICO.** Organisations face a duplicative process of having to go through the same BCR approval procedure in the EU and the UK. However, there is no difference in the requirements. An informal mutual recognition already works with respect to Switzerland. Finally, and in the longer term, the EDPB should explore how to recognise (fully or partly) BCRs approved outside the EU under data protection laws similar to GDPR (e.g. Brazil, Singapore, and Australia).

c) **The EDPB should explore how to evolve and expand the utility of BCR as a data transfer mechanism, as provided by GDPR, between undertakings engaged in joint economic activities.** During the negotiations on the EU GDPR, this provision was interpreted to mean that companies/ corporate groups that are engaged in joint economic activity, such as a joint venture or an outsourcing or other service contract, may be able to benefit from each other's BCR to legitimise transfers between the two groups. Legally and logically, there should not be any obstacles for one corporate group with an approved BCR-C to share data with another corporate group also with an approved BCR-C in the context of commercial and economic activity. Both corporate groups have, through their respective BCRs, committed to a uniform and high level of data protection for any data they process within the group.

d) Ideally, and in the long run, BCR could and should evolve further. **BCR should not require prior approval by DPAs, as it is currently understood. Instead, BCR should be based on final DPA approval after a review by a third party—an accredited certification body under the GDPR or an "Accountability Agent" as in the APEC CBPR system.** One can imagine even a step further, where BCR would be based on a self-certification system similar to that of Privacy Shield. A third-party review system could meet the DPA approval requirement in Article 47(1) GDPR. Augmenting the BCR process with such a third-party review process would ease the current burden on DPA resources for approving BCR and facilitate faster BCR processing times.

   However, for the time being, Article 47(1) is interpreted to mean that BCR be entirely approved by a competent authority directly and without the assistance of a third-party Accountability Agent. Therefore, all efforts should be made to ensure that the BCR review, approval and documentation process is made as scalable, affordable and accessible to as many organisations as possible. Organisations considering BCR should not be disadvantaged and put in a less competitive position than those relying on other data transfers mechanisms, such as SCCs.

***

In the context of the draft Recommendations 1/2022, the EDPB should:

- Allow BCR-C holders, specifically the Group's data exporters, to consider the same elements provided under Sections 33 and 43.3 in Recommendations 01/2020 and the flexibility provided under Footnote 12 of the SCCs clause 14 before carrying out a transfer of personal data to a BCR member outside the EEA;
- Revise Section 5.3 of Annex 2 to clarify that the BCR-C Group may consolidate the accountability requirements;
- Allow BCR-C holders to designate a single method for submitting individuals requests and complaints (e.g. a ticketing system);
- Revise Section 1.3.1 to allow the BCR-C group to communicate the substantive or material changes in the publicly published version of the BCR; and
- Streamline the BCR documentation requirements.

***

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@HuntonAK.com, Markus Heyder, mheyder@HuntonAK.com, Natascha Gerlach, ngerlach@HuntonAK.com or Laila Abdelaziz, labdelaziz@HuntonAK.com.

***

ANNEX: - DETAILED COMMENTS IN RESPONSE TO DRAFT RECOMMENDATIONS 01/2022

Draft Recommendations	Content	Concern / Suggestion
Introduction, para. 5	BCR-C are suitable for framing transfers of personal data from controllers covered by the geographical scope of the GDPR pursuant to Article 3 GDPR to other controllers or to processors (established outside the EEA) within the same Group . . . Hence, the obligations set out in BCR-C apply in relation to entities within the same Group acting as controllers and to entities acting as 'internal' processors.	The Recommendations do not take into account the case where the data importer is established in a jurisdiction recognised as adequate by the European Commission. It would be helpful if the Recommendations could address this clarification.
Introduction, para. 13	The EDPB expects all BCR-C holders to bring their BCR-C in line with the requirements set out below. This includes BCR-C that have been approved before the publication of these Recommendations. Such changes will have to be done in compliance with the commitments taken in their BCR-C in accordance with Section 5.1 below.	This requirement does not include a timeframe for current BCR-C holders, that should be given a reasonable amount of time and notice to make any necessary changes.
1.3.1 Creation of third-party beneficiary rights that are enforceable by data subjects.	- Duty to inform the data subjects about any update of theBCR-C and of the list of BCR members (see Section 8.1 below);	This requirement is not sufficiently clear. The Recommendations should clarify in which scenarios controllers must inform data subjects of changes. Section 8.1 deals with notification to the SA and not to data subjects. If this requirement is maintained in the final version, it should be clearly defined as a duty to update the published version of the BCR. Anything else would be burdensome for the BCR holder and a nuisance to the data subject.
1.3.1 Creationof third-party beneficiary rights that are enforceable by data subjects.	The Group needs to make sure that third-party beneficiary rights are effectively created to make those commitments binding (see Section 1.2 below).	The reference to "Section 1.2" seems to be an error.

1.7 Easy access to the BCR-C for data subjects	The BCR-C must contain the commitment that all data subjects should be provided with information on their third-party beneficiary rights with regard to the processing of their personal data and on the means to exercise those rights.	This is often included as part of the privacy policy. The deletion of the reference to GDPR Articles 13 and 14 implies that this will not be sufficient. If the intent is to include this in the published version of the BCR-C, it should be clearly stated.
1.7 Easy access to the BCR-C for data subjects	Furthermore, the BCR-C must contain the commitment that data subjects will be provided at least with the description of the scope of the BCR-C (see Section 2 below), the clause relating to the Group's liability (see Section 1.4 above), the clauses relating to the data protection principles (see Section5.1.1 below), to the lawfulness of the processing (see Section 5.1.2 below), to security and personal data breach notifications (see Section 5.1.3 below), to restrictions on onward transfers (see Section 5.1.4 below), and the clauses relating to the rights of the data subjects (see Section 5.2 below). This information should be up-to-date and presented to data subjects in a clear, intelligible, and transparent way. This information should beprovided in full, hence a summary hereof will not be sufficient.	The scope described under Section 2 is too broad for data subject communication. Allowances should be made to describe the scope in more general terms. Detailed descriptions of processing activities, as currently provided under Section 2, have the potential to lead to "notice fatigue" on the side of individuals and are an administrative burden for organisations. We suggest including further clarification regarding how to provide all the required information to data subjects in a way that does not create "notice fatigue" for data subjects. The last sentence in this requirement states that the information should be provided "in full" so that a summary would seemingly not be sufficient. It is not clear, however, what constitutes "in full"; further clarification on this summary and its level of detail is needed. A balance should be struck between providing sufficient transparency about the BCRs and making the information accessible and easy to understand for the data subjects.
1.7 Easy access to the BCR-C for data subjects	In case the Group plans to not publish the BCR-C as a whole but only certain parts or a specific version aimed at informing data subjects, the Group should expressly provide in the BCR-C the list of the elements that it will include in that public version. In such a situation, the description of	The level of detail on the scope, as provided in Section 2, is likely too granular for individuals, and more flexibility should be allowed with respect to the description of the scope under the published BCR documents. Individuals should be provided information that impacts their rights and

	the material scope of the BCR-C should always be part of the information on the BCR- C that is publicly available. The list of definitions (see Section 9.1 below) and, if applicable, of abbreviations which are used in the BCR-C should, in any case, be included in the parts of the BCR-C which are published. The BCR-C should contain an express commitment in this regard.	freedoms, without being inundated with granular levels of information that can cause notice fatigue.
1.7 Easy access to the BCR-C for data subjects	The BCR-C must use clear and plain language so that_employees and any other person in charge of applying the BCR-C can sufficiently understand them. The same applies to_any parts/version of the BCR-C that will be published with the aim of providing access to the BCR-C for data subjects.	This requirement makes sense for the public version of the BCRs but not for the Intercompany Agreement or other documentation about compliance that is meant to be technical.
2.1 Description of the material scope of the BCR-C	In order to be transparent as to the scope of the BCR- C, the BCR-C must specify their material scope and therefore contain a description of the transfers.	Further clarification on the level of detail of this description needs to be provided. A balance should be struck between providing sufficient transparency and making the information accessible and easy to understand for individuals.
2.2 List of BCR members, and description of the geographical scope of the BCR-C	The BCR-C shall specify the structure and contact details of the Group and of each of its BCR members (contact details of the BCR members – such as address and company registration number, where available – should be inserted in the list of BCR members that is part of the BCR-C, for example, an annex thereof, that has to be published along with the BCR-C).	Including information so specific such as registration numbers, may be excessive and unnecessary to exercise data protection rights. This only adds an administrative burden for organisations and should be deleted.
3.2 Complaint handling process for the BCR-C	The BCR-C (or, depending on the case, the parts of the BCR-C that will be published for the attention of data subjects, see Section 1.7 above) will include the point(s) of contact where data subjects can lodge any complaints related to the processing of their personal data covered by the BCR-C. A single point of contact or a number of points of contact are possible. In this regard, a physical address should be provided. Additionally, further contact options may be provided, e.g. a generic e-mail address and/or a phone number.	While providing a means for individuals to contact the BCR organisation is of obvious importance, providing an email address can actually be detrimental. Publicly posted email addresses become the target of spammers for purposes not related to data protection, which creates an additional burden on the DPO and privacy offices. The part of the organisation tasked with addressing data subject requests may instead implement appropriate contact tools that

	While data subjects are encouraged to use the point(s) of contact indicated, this is not mandatory.	allow for traceability and follow-up (for instance, a ticketing system). This allows for a higher degree of responsiveness than an email address. Therefore, we recommend eliminating the reference for email addresses and phone numbers. At the least, organisations should be able to provide web forms as an acceptable option. Additionally, we caution the EDPB against creating a de facto incentive for individuals to lodge complaints before via any available channel. This raises uncertainty and can become an impediment to an efficient and timely response. We suggest removing this from Section 3.2.
3.3 Audit programme covering the BCR-C	Data protection officers should not be the ones in charge of the BCR-C if such a situation can result in a conflict of interest. Functions that may possibly be entrusted with deciding on the audit plan/programme and/or with conducting audits include, for instance, Audit Departments, but other appropriate solutions may be acceptable too, provided that: - the persons in charge are guaranteed independence as to the performance of their duties related to these audits; and - the BCR-C include an explicit commitment in this regard."	This requirement is too restrictive considering that Article 39 GDPR defines tasks of the DPO to include monitoring "compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits". Moreover, the involvement of the DPO in an audit is crucial to evidence the monitoring of compliance with the BCRs. Additionally, the DPO is an independent function in many organisations, so the problem of conflict of interest should not be an issue.

3.3 Audit programme covering the BCR-C	It is not mandatory to monitor all aspects of the BCRC each time a BCR member is audited, as long as all aspects of the BCR-C are monitored at appropriate regular intervals for that BCR member.	This requirement does not consider that some organisations may have a centralised function for data protection that services all members of the group. The audit requirements should apply to the members who need to implement certain aspects locally but, in general, to the application of the requirements overall for the group. Additionally, BCR organisations should be able to leverage audits done for other purposes or mechanisms as long as the requirements align. When getting a certification, for instance, the certification requirements might overlap with BCR requirements and duplicating an audit process is an unnecessary strain on resources. The elements and principles should recognise the ability to meet requirements for multiple mechanisms on a single review mechanism.
3.4 Creation of a network of data protection officers (DPOs) or appropriate staff for monitoring compliance with the BCR-C	The DPO should not have any tasks that could result in a conflict of interest. The DPO should not be in charge of carrying out data protection impact assessments, neither should they be in charge of carrying out the BCR-C audits if such situations can result in a conflict of interests. However, the DPO can play a very important and useful role in assisting the BCR members, and the advice of the DPO should be sought for such tasks.	This requirement is too restrictive. Article 35 GDPR expressly requires the controller to seek the advice of the DPO when carrying out an impact assessment. More guidance is needed regarding when a DPO is seen as "in charge" of carrying out impact assessments. Additionally, the DPO is an independent function in many organisations, so the problem of conflict of interest should be an exception.
5.1.2 Lawfulness of processing	The BCR-C should contain an exhaustive list of all legal basis for processing which the BCR members intend to rely on. Only legal basis as those stipulated in Article 6(1) and (3) GDPR, or in other legal basis laid down in Union or Member state law, as permitted by the GDPR, can be used.	This requirement does not add substantial protection. As organisations do not know all possible business scenarios (they may develop and constantly innovate in products and services), it is likely that organisations will include any possible legal basis to anticipate all scenarios and not have to

		modify the BCRs. It seems an unnecessary requirement.
5.1.3 Security and personal data breach notifications	The BCR-C should include a commitment to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk(s) for the rights and freedoms of natural persons (see Article 5(f) and Article 32 GDPR). It is not mandatory to copy-paste the wording of such GDPR provisions. However, the BCR-C need to create those obligations in a sufficiently elaborated manner that is in line with the content of these provisions.	Such technical and organisational measures may be defined by some large organisations in other documentation, such as their Data Breach Notification Guide, which is an extensive document separated from the BCR documentation. We suggest adapting this section from the referential, so it makes clear that in such a case, the whole guide does not need to be included in the BCR documents but that a description and a link to the document and its location are enough.
5.4.1. Local laws and practices affecting compliance with the BCR-C	The BCR-C shall contain a clear commitment that BCR members will use the BCR-C as a tool for transfers only where they have assessed that the law and practices in the third country of destination applicable to the processing of the personal data by the BCR member acting as data importer, including any requirements to disclose personal data or measures authorising access by public authorities, do not prevent it from fulfilling its obligations under these BCR-C.	It is unclear what timeframes organisations have to re-assess when national laws change. An appropriate and sufficient timeframe for assessing new regulations should be provided.
5.4.2 Obligations of the data importer in case of government access requests	iv. The data importer will preserve the abovementioned information for as long as the personal data are subject to the safeguards provided by the BCR-C and shall make it available to the Competent SAs upon request.	No timeframe is defined for providing the mentioned information. Due to the fact that this information can be in languages different from the data subject's language, it might take considerable amounts of time to get all information translated in order to make it available to the competent SAs.

8.1 Process for updating the BCR-C.	The BCR-C should impose a duty to report changes, including to the list of BCR members, without undue delay, to all BCR members.	We suggest specifying that minor changes should be communicated to all BCR members on a specific period of time (e.g. annually) instead of requiring all changes to be communicated without undue delay. Major changes should be communicated to participating members as soon as practical.
8.1 Process for updating the BCR-C.	Where a modification to the BCR-C would possibly be detrimental to the level of the protection offered by the BCR-C or significantly affect them (e.g. changes to the binding character, change of the Liable BCR member(s)), it must be communicated in advance to the SAs, via the BCR Lead, with a brief explanation of the reasons for the update. In this case, the SAs will also assess whether the changes made require a new approval.	Further examples of what changes would be considered significant in this context would be welcome.
8.1 Process for updating the BCR-C.	Any other changes to the BCR-C or to the list of BCR members should be notified once a year to the SAs, via the BCR Lead, with a brief explanation of the reasons for the update. This includes any changes made in order to align the BCR-C with any updated version of these EDPB Recommendations.	We suggest including "significant" in "other changes" so it is clear that this requirement refers to the data protection program and not to minor style or typographic corrections to the BCR documentation.