Recommendations 1/2026 on the Application for Approval and on the elements and principles to be found in Processor Binding Corporate Rules (Art. 47 GDPR)

Adopted on 15 January 2026

VERSION HISTORY

Version 1	15 January 2026	Adoption for public consultation

Table of contents

The European Data Protection Board

Having regard to Article 70(1)(i) of the Regulation 2016/679/EU of the European Parliament and of the Council 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, (hereinafter "**GDPR**"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Articles 12 and 22 of its Rules of Procedure,

Has adopted the following recommendations:

1 Introduction

1.1 General information

1. The GDPR expressly provides for the use of Binding Corporate Rules (hereinafter "**BCR**") by a group of undertakings, or a group of enterprises engaged in a joint economic activity (hereinafter "**Group**") for transfers of personal data in the sense of Article 44 GDPR.[2]

2. On 6 February 2018, the Article 29 Working Party (hereinafter "WP29") adopted a table with the elements and principles to be found in Processor BCR (hereinafter "BCR-P") in order to reflect the requirements referring to BCR-P (hereinafter "WP257 rev.01"). The European Data Protection Board (hereinafter "EDPB") endorsed WP257 rev.01 on 25 May 2018. These Recommendations also repeal and replace WP257 rev.01, while in substance building on it.

[1] References to "**Member States**" made throughout this document should be understood as references to "EEA Member States". Likewise, references to the "Union" or "EU" should be understood as references to the "EEA".

[2] Article 47(1)(a) and (2)(a) GDPR; see also Recital 110 of the GDPR.

3. On 11 April 2018, the Article 29 Working Party (thereinafter “WP29”) adopted Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data (hereinafter: “**WP265**”). The European Data Protection Board (hereinafter “EDPB”) endorsed WP265 on 25 May 2018. These Recommendations repeal and replace WP265, while in substance building on it.

4. These recommendations are meant to:

   - Provide a standard form for the application for approval of BCR for processors (hereinafter **“BCR-P”**);
   - Clarify the necessary content of BCR-P as stated in Article 47 GDPR;
   - Distinguish between what must be included in BCR-P and what must be presented to the BCR Lead supervisory authority (hereinafter “**BCR Lead**”)[3] in the BCR application; and
   - Explain and elaborate on the requirements.

5. Pursuant to Article 46(2)(b) GDPR, BCR are a tool for providing appropriate safeguards for transfers of personal data to third countries that have not been recognised as providing an adequate level of protection pursuant to Article 45 GDPR. BCR should create enforceable rights and set out commitments in order to create, for the personal data transferred under the BCR, a level of protection essentially equivalent to the one provided by the GDPR. It is therefore not sufficient for the BCR-P to make a reference to the GDPR, but the BCR-P must rather expressly set forth and reflect within the group the requirements envisaged by the GDPR.

1.2 Scope of BCR-P

6. BCR-P apply to data that will be processed by members of the Group covered by the geographical scope of the GDPR pursuant to article 3 GDPR acting as processors on behalf of a controller **that is not a member of the Group**, and which are then transferred by such processors to and processed by Group members as sub-processors in third countries, including any onward transfers to other BCR members in third countries. Hence, the obligations set out in BCR-P apply to entities within the same Group acting as processors and to entities acting as ‘internal’ sub-processors.[4] BCR-P are, however, not suitable to cover a direct transfer from an external controller[5] covered by the geographical scope of the GDPR to one of the processors members of the BCR-P Group in third countries. For such a transfer, a different transfer tool under Article 46 is required instead.

[3] See EDPB Document Setting Forth a Co-Operation procedure for the approval of Binding Corporate Rules for controllers and processors, of 13/03/2025, paras. 7 et seq, available at https://www.edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-setting-forth-co-operation-procedure-approval_en.

[4] Throughout this document, the term «internal (controller or processor/sub-processor)» is used to label a controlle/processor/sub-processor that is a member of the BCR-P Group.

[5] Throughout this document, the term „external (controller or processor/sub-processor)“ is used for labeling a controller/processor/sub-processor that is not a member of the BCR-P Group.

7. By contrast, BCR for controllers (hereinafter: "BCR-C") are suitable for framing transfers of personal data from controllers covered by the geographical scope of the GDPR[6] to other controllers or to processors within the same Group established in third countries.[7]

1.3 Interplay between BCR-P and processing agreement

8. In addition to the BCR-P, a contract or other legal act under Union or Member State law, which is binding on the processor with regard to the controller and comprises all elements as required by Article 28(3) GDPR,[8] must be signed by the external controller with one or several of the members of the BCR-P Group that are covered by the geographical scope of the GDPR.[9] Such contract or other legal act (referred here as the processing agreement) should include a reference to the BCR-P and make the BCR-P enforceable for the controller against the members of the Group.[10] While not itself an integral part of the BCR-P, a template of such processing agreement or other legal act that the Group intends to use can be requested by the BCR Lead from the applicant during the approval procedure.

9. The BCR-P, for their part, are also aimed to fulfil the requirements of Article 28 (4) of the GDPR where a processor within the group engages another internal processor for carrying out specific processing activities on behalf of the controller.[11] A Member that has implemented BCR for Processors will hence not need to sign a sub-processing agreement with each of the sub-processors part of the BCR-P Group.[12]

10. EU data protection legislation applicable to members of the Group must be complied with and cannot be overruled by provisions in the BCR-P unless the BCR-P voluntarily provide for a higher level of protection. The processing agreement entered into between the controller and the processor(s) should not be in contradiction with or lower the protection provided by the BCR-P.

[6] Please note that at least one group member in the EEA is required (see Chapter 3, Section 1.4 of these Recommendations).

[7] See EDPB 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), Introduction, Par. 5.

[8] Please note that, while the BCR-P only need to include a general description of the envisaged transfers that may be carried out under the BCR-P, this does not limit the controller's, the processor's and any sub-processor's obligations to describe in each processing agreement and sub-processing agreement the covered processing with the degree of specificity (subject-matter and duration of processing, nature and purpose of the processing, type of personal dasta, categories of data subjects) as mandatorily required by Article 28(3) GDPR (see Chapter 3, Sect. 2.1 for details).

[9] As for the geographical scope of the GDPR, see Article 3 GDPR. Please note that at least one Group member in the EEA is required (see Footnote 8).

[10] As for the enfoceability by the controller see Section 1.3.2 of Chapter 3 of this paper (« Elements and Principles to be included in BCR-P »).

[11] This is exactly the scenario for which BCR-P are aimed for, see Par. 6.

[12] However, in accordance with Article 28(4) and Art. 28(3)(a) GDPR, Group members signing a contract or other legal act as processors with the controller as per Article 28 Par. 3 GDPR must pass on the instructions of the controller to any Group member sub-processors to which they disclose data on behalf of the controller. See Section 2.1 of Chapter 3 of this paper with regards to the need to describe the covered processing activities vis-á-vis each sub-processor. Moreover, see Section 5.1.1 of Chapter 3 of this paper as to certain obligations to be included in the BCR-P in this regard.

1.4 Scope of approval decision

11. BCR are subject to approval[13] by the BCR Lead. In this respect, it is worth highlighting the difference between the BCR Lead – which is competent for issuing the approval of the BCR[14] - and the SA which is competent for the controller on behalf of which a specific transfer covered by the BCR-P is carried out, and also the SA which is competent for the specific processor that acts as exporter carrying out a specific transfer (on behalf of the controller) under that BCR-P.[15]

12. The draft approval decision of the BCR Lead is subject to an opinion by the EDPB[16]. The approval confirms that the requirements set out in Article 47 GDPR are met, and therefore, that the commitments included in the BCR provide for appropriate safeguards in the sense of Article 46 GDPR.

13. However, an approval of the BCR-P does not amount to a confirmation that the specified processing activities effectively comply with the conditions set out in the BCR in practice, nor does it include an assessment of compliance of those processing activities covered by the BCR-P which fall under the GDPR with all of the requirements of the GDPR as applicable to them.[17] It is therefore the responsibility of both the Group Members to which the GDPR applies as regards a transfer carried out under the BCR-P, and the respective controllers covered by the GDPR to ensure that they comply with all requirements of the GDPR as applicable to processing activities and transfers covered by the BCR-P. For example, it is the responsibility of the processor and the relevant controller on behalf of which it transfers personal data to assess for each transfer, on a case-by-case basis, whether there is a need to implement supplementary measures in order to provide for a level of protection essentially equivalent to the one provided by the GDPR.[18] The responsibility for implementing such supplementary measures (if needed with the help of the data importer) lies with each data exporter (i.e. the processor), while the controller on behalf of which the personal data are transferred has the responsibility to verify them.[19] Such supplementary measures are not assessed by supervisory authorities (hereinafter "**SAs**") as part of the process of approval of the BCR-P.

[13] In accordance with Article 47(1) GDPR.

[14] See EDPB Document Setting Forth a Co-Operation procedure for the approval of Binding Corporate Rules for controllers and processors, of 13/03/2025, paras. 7 et seq, available at https://www.edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-setting-forth-co-operation-procedure-approval_en.

[15] Throughout these Recommendations, the term "Competent SA(s)" refers to both the data protection SA(s) competent for the processor(s) acting as data exporter(s) of the specific transfer(s), and also to the data protection SA(s) competent for the controller(s) on behalf of which the specific transfer(s) is/are carried out.

[16] In accordance with Article 46(4), Article 64(1)(f) and Article 64(3) GDPR.

[17] It should be recalled that BCR-P apply, among others, to personal data that are processed by members of the Group covered by the geographical scope of the GDPR pursuant to article 3 GDPR acting as processors (see Par. 6), so the GDPR applies to data covered by the BCR-P when these data are processed and transferred under the BCR-P by these Group members.

[18] See Chapter 3 of these Recommendations, Section 8.1, and EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

[19] See EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Version 2.0, Par. 19: "… the processor acts as a data exporter on behalf of the controller and has to ensure that the provisions of Chapter V are complied with for the transfer at stake according to the instructions of the controller, including that an appropriate transfer tool is used. Considering that the transfer is a processing activity carried out on behalf of the controller, the controller is also responsible and could be liable under Chapter V …".

14. Groups may use the BCR-P as their global data protection policy governing processing by all entities bound (either exporters or importers) acting as processors or sub-processors whatever their location (inside or outside the EEA).[20] Notwithstanding this possibility, the scope of the BCR approval by the BCR Lead is always limited to transfers of personal data from entities under the scope of application of the GDPR to third countries that have not been recognised as providing an adequate level of protection pursuant to Article 45 GDPR, and their onward transfers to other Group members bound by the BCR (hereinafter "**BCR member(s)**").

15. Once approved, BCR-P can be used for transfers from all relevant Member States. The SA competent for the data exporter and also the SA competent for the controller on behalf of which the transfer is carried out will be competent to assess the adherence to the BCR by the data importer in the third country in relation to the relevant transfers.

1.5 Update of existing BCR-P

16. These Recommendations become effective on the date of the publication of the final version after public consultation.

17. Consequently, the EDPB expects all new and ongoing BCR-P applicants to bring their BCR-P in line with the requirements set out below. BCR-P applications that by the time these recommendations are published have already reached the stage of a "consolidated draft" in accordance with Par. 15 of the "EDPB Document Setting Forth a Co-Coperation procedure for the approval of Binding Corporate Rules for controllers and processors" of 13/03/2025 (the "EDPB document on the Co-Operation procedure for BCR")[21] and for which the EDPB also issues its opinion by the end of [*placeholder - to be completed in final version*] will have to bring their BCR in line with these recommendation with their [*placeholder - to be completed in final version*] annual update.

18. All BCR-P holders must also comply with these Recommendations. Related changes will have to be done as part of their annual update. In line with Chapter 3, Section 11 of this document, such update will not generally trigger the need for a new approval since they are meant to improve the safeguards for data subjects.

19. The BCR Lead SAs will be ready to provide, where needed, additional information upon request.

[20] Such global policy, if any, should not derogate in any way from the minimum level of protection as provided for by the GDPR for the processing of personal data transferred from entities under the scope of application of the GDPR.
[21] Available at https://www.edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-setting-forth-co-operation-procedure-approval_en.

2 Application form

2.1 General Instructions for Applicants:

- Only a single copy of the form need be filled out and submitted to the Supervisory Authority (‘SA’) you consider to be the BCR Lead in accordance with Articles 47(1) and 64 GDPR and the EDPB document on the Co-Operation procedure for BCR ; this form may be used in all EEA Member States.
- In case of an application for a BCR-C and a BCR-P, separate forms need to be filled out for each BCR.
- Please fill out all entries of **Part 1** of the application form and submit the form to the SA you consider to be the BCR-P Lead. As soon as a decision on the BCR Lead has been made[22], the BCR Lead will determine when it will invite you to fill out and submit **Part 2** of the application form including its Annexes.
- You may attach additional pages or annexes if there is insufficient space to complete your responses.
- You may indicate any responses or materials that is in your opinion commercially sensitive and should be kept confidential but, in any case, be aware that the relevant document will be shared among the concerned SAs and the EDPB which, under Article 64 GDPR, has to issue its opinion on the approval draft decision of your BCR-P. Requests by third parties for disclosure of such information, will, however, be handled by each SA involved in accordance with national legislation.
- The next steps of the procedure are described in the EDPB document on the Co-Operation procedure for BCR.
- BCR holders notifying the update of their BCR-P only need to sign Part. 1, Section 4 (“Acknowledgment”) of the Application Form below.
- BCR holders must in the course of their annual update (see Section 11 of Chapter 3 of this Recommendations document) confirm sufficient assets pursuant to Part 2, Section 5 (“Assets”) of the Application Form below.

[22] See EDPB Document Setting Forth a Co-Operation procedure for the approval of Binding Corporate Rules for controllers and processors, of 13/03/2025, paras. 12 et seq.

2.2 Instructions for Filling in Part 1 (applicant information):

2.2.1 Section 1: Structure and Contact Details of the Applicant and of the Group

- If the Group has its headquarters in the EEA the form should be filled out and submitted by that EEA entity or, under certain circumstances, another EEA entity with delegated data protection responsibilities[23]. In the latter case, the Group should provide additional justification as to why another EEA entity which is not the EEA headquarters is the applicant.
- If the Group has its headquarters outside the EEA, then the Group should appoint a Group entity located inside the EEA as the Group member with delegated data protection responsibilities. This is the entity which should then submit the application on behalf of the Group.
- Contact details for queries:
    - Please indicate a contact (including contact information) to whom queries may be addressed concerning the application.
    - This contact does not need to be located in the EEA, although this is advised for practical reasons.
    - You may indicate a function rather than a specific person.

2.2.2 Section 2: Short description of expected/anticipated data flows

- The applicant should provide a brief description of the scope and nature of the data flows to third countries for which approval is sought.

2.2.3 Section 3: Determination of the BCR Lead

- In accordance with Article 64 GDPR, the BCR Lead is the authority in charge of coordinating the approval of your BCR-P, which then could be considered appropriate safeguards for transfers of personal data by BCR-P Group members to third countries, without requiring any specific authorisation for the use of the BCR-P from the other SAs concerned.

[23] According to Article 47(2)(f) GDPR, there should always be an EU based member of the group established on the territory of a Member State accepting liability for any breaches of the BCR-P by any member concerned not established in the EEA. If the headquarters of the group are established outside the EEA these responsibilities shall be delegated to a member based in the EEA.

- Before approaching one SA as the presumptive BCR Lead, please examine the factors listed in par. 8 of the EDPB Document Setting Forth a Co-Operation procedure for the approval of Binding Corporate Rules for controllers and processors of 13/03/2025.[24] Based on these factors you should explain in Part 1/Section 3 of the Application Form below which SA should be the BCR Lead. The SAs are not obligated to accept the choice that you make if they believe that another SA is more suitable to be BCR Lead, in particular if it would be worth for speeding up the procedure (e.g. taking into account the workload of the originally requested SA).

Application form for approval of processor binding corporate rules (“BCR-P”)

Part 1: Applicant Information

1. STRUCTURE AND CONTACT DETAILS OF THE GROUP OF UNDERTAKINGS OR GROUP OF ENTERPRISES ENGAGED IN A JOINT ECONOMIC ACTIVITY (THE GROUP)

Name of the Group and location of its headquarters:

Does the Group have its headquarters in the EEA?
□ Yes
□ No

Name and location of the applicant:

Identification number (if any):

Legal nature of the applicant (corporation, partnership, etc.):

Description of position of the applicant within the Group:
(e.g. headquarters of the Group in the EEA, or, if the Group does not have its headquarters in the EEA, the member of the Group inside the

[24] Available under https://www.edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-setting-forth-co-operation-procedure-approval_en.

EEA with delegated data protection responsibilities)

Name and/or function of contact person (note: the contact person may change, you may indicate a function rather than the name of a specific person):

Address:

Country:

Phone number: E-Mail:

EEA Member States from which the BCR-P will be used:

2. SHORT DESCRIPTION OF PROCESSING AND DATA FLOWS[25]

Please, indicate the following:

- Expected nature of the data covered by the BCR-P, and in particular, if they apply to one category of data or to more than one category, the type of processing and its purposes, the types of data subjects affected (for instance, data related to employees, customers, suppliers and other third parties as part of their respective regular business activities…), anticipated types of processing and its purposes

- Do the BCR-P only apply to transfers from the EEA, or do they apply to all transfers between members of the group acting as processors and transferring data to other members of the group acting as sub-processors?

- Please specify the EEA state from which most of the data are transferred outside the EEA on the basis of the BCR-P

- Extent of the transfers within the Group that are covered by the BCR-P; including a description and the contact details of any Group members in the EEA or outside the EEA to which personal data may be transferred on the basis of the BCR-P

[25] See Article 47(2)(a) and (b) GDPR.

3. DETERMINATION OF THE LEAD SUPERVISORY AUTHORITY ('BCR LEAD')[26]

Please explain which should be the BCR Lead, based on the following criteria:

- Location of the Group's EEA Headquarters

- If the Group is not headquartered in the EEA, the location in the EEA of the Group entity with delegated data protection responsibilities

- The location of the company which is best placed (in terms of management function, administrative burden, etc.) to deal with the application and to enforce the BCR-P in the Group

- EEA Member States from which most of the transfers outside the EEA will take place

4. ACKNOWLEDGEMENT

We acknowledge on behalf of each member of the Group that

- each BCR member ensures that all requirements set out in GDPR (including, but not limited to Chapter V) and BCR-P, as applicable to processors, are met for each transfer;

-before carrying out any transfer of personal data on the basis of the approved BCR-P to one of the BCR-P members of the Group, it is the responsibility of any Group member acting as data exporter, if needed with the, to assess whether the legislation of the third country of destination does not prevent the recipient from complying with the BCR-P, including with regard to onward transfer situations. This assessment has to be conducted in order to determine whether any legislation or practices of the third country, applicable to the to-be-transferred data go beyond what

[26] See Part 1, WP 263.

is necessary and proportionate in a democratic society to safeguard important public interest objectives recognized by the Union, in particular criminal law enforcement and national security and may impinge on the data importer's and/or the data exporter's ability to comply with their commitments taken in the BCR-P, taking into account the circumstances surrounding the transfer. In case of such possible impingement, the data exporter in an EEA Member State, if needed with the help of the data importer, should assess whether it can provide supplementary measures in order to exclude such impingement and therefore to nevertheless ensure, for the envisaged transfer(s) at hand, an essentially equivalent level of protection as provided in the EU. The controller on behalf of which the personal data are transferred has the responsibility to verify the supplementary measures taken by the processor acting as exporter.[27] Such supplementary measures are not assessed by supervisory authorities (hereinafter "SAs") as part of the process of approval of BCR-P.

In any case, where the data exporter is not able to implement supplementary measures necessary to ensure an essentially equivalent level of protection as provided in the EU, personal data cannot be lawfully transferred to a third country under the BCR-P. In the same vein, where the data exporter is made aware of any changes in the relevant third country legislation that undermine the level of data protection required by EU law, the data exporter is required to suspend or end the transfer of personal data at stake to the concerned third countries.[28]

Date, Signature of the applicant (Board level)

[27] See EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Version 2.0, of 14/02/2023, par. 19.

[28] It should be recalled that aside from the processor (member of the Group) acting as exporter, the same obligation applies in this case to the controller on behalf of which the data transfer takes place.

5. BINDING NATURE OF THE BCR-P

Binding within the entities of the Group

How are the BCR-P made binding upon the members of the Group?

□ Intra Group Agreement

□ Unilateral Declaration (hereinafter: UD) if the requirements set out in Section 1.2 of the “Elements and principles” part (= Chapter 3) of these EDPB Recommendations are met

□ Other means (only if the Group demonstrates how the binding character of the BCR-P is achieved), please specify

Please attach the draft Intra Group Agreement / UD / “other means”. Please note that these documents will have to be signed at Board level after the BCR-P approval has been obtained.

Please explain the legal basis enabling the member(s) of the Group with delegated data protection responsibility to enforce the BCR-P obligations of other members of the Group (e.g. rights of a parent company residing in corporate law):

Does the internally binding effect of your BCR-P extend to the whole Group? (If some Group members should be exempted, specify how and why)

Binding upon the employees

Your Group may take some or all of the following steps to ensure that the BCR-P are binding on employees, but there may be other steps. Please, give details below.

□ Individual and separate agreement(s) / undertaking with sanctions;

□ Clause in employment contract with a description of applicable sanctions;

□ Collective agreements with sanctions;

□ Internal policies with sanctions (but the Group must properly explain how the BCR-P are made binding on employees);

□ Other means (but the Group must properly explain how the BCR-P are made binding on employees)

Please provide a summary, supported by extracts as appropriate, to explain how the BCR-P are binding upon employees.

Assets
Please confirm that the liable BCR-P member(s) established on the territory of an EEA Member State (e.g. the European headquarters of the Group, or the member of the Group with delegated data protection responsibilities in the EEA) has made appropriate arrangements to enable itself payment of compensation for any damages resulting from the breach of the BCR-P by BCR members outside the EEA, and explain how this is ensured.

6. EFFECTIVENESS

It is important to show how the BCR-P in place within your organization are brought to life in practise, in particular in non-EEA countries where data will be transferred on the basis of the BCR-P, as this will be significant in assessing the adequacy of the safeguards. Please provide information on the elements below.

Training and awareness raising (employees)

- Special training programs (it is necessary to include information about the frequency/regularity of these programs and additional information that underpins and serves as evidence; the BCR Lead may ask for additional evidence if deemed necessary)

- Employees are tested on BCR and data protection (it is necessary to include information about the frequency of tests as well as additional information that underpins and serves as evidence; the BCR Lead may ask for additional evidence if deemed necessary)

- BCR are communicated to all employees on paper or online

- Review and approval by senior officers of the company

- How are employees trained to identify the data protection implications of their work, i.e. to identify that the relevant privacy policies are applicable to their activities and to react accordingly? (This applies whether these employees are or not based in the EEA)

Network of data protection officers (DPO) or appropriate staff

Please confirm that a network of DPOs or appropriate staff (such as a network of privacy officers) is appointed with top management support to oversee and ensure compliance with the BCR for Processors:
Please explain how your network of DPOs or privacy officers functions: - Internal structure: - Role and responsibilities:

Date, Signature of the applicant (Board level)
(please also indicate name, position, and contact details)

Annex 1: copy of the BCR-P

Please attach a copy of your BCR-P to your application. Please note that all mandatory content needs to be included in the BCR documents (in the core document(s) or its annexes), while “supporting documents” (i.e. documents that are not part of the BCR) may only be submitted for reasons of further explanation[29].

Annex 2: copy of the filled-out table “elements and principles to be found in BCR-P”

Please fill out the table “Elements and Principles to be found in BCR-P” and attach it to your application.

[29] Please note that any documents that are submitted may be subject to access requests based on freedom of information legislation, as applicable.

3 Elements and principles to be found in BCR-P

Criteria for BCR-P approval	In BCR-P	In application form	Reference	Comments	References to BCR-P, application form BCR-P, and / or supporting documents[30]
1 - BINDING NATURE AND RELATED ASPECTS					
Internal binding nature					
1.1 Duty to respect the BCR-P	YES	NO	Article 47(1)(a) and (2)(c) GDPR[31]	The BCR-P must be legally binding and should contain a clear duty for each BCR member, including their employees, to respect the BCR-P. The BCRs shall also expressly state that each BCR member including their employees shall respect the instructions from the controller regarding the data processing and the security and confidentiality measures as provided in the processing agreement (see Art. 28, 29 and 32 of the GDPR).	
1.2 Explanation of how the BCR-P are internally[32] made binding on the BCR	NO	YES	Article 47(1)(a) and (2)(c) GDPR	The Group will have to explain in its application form how the BCR-P are made binding:	

[30] To be completed by the applicant by inserting references to the paragraphs/sections/parts of the BCR documents and, if necessary, any supporting documents, that address the respective requirement. Please note that all mandatory content needs to be included in the BCR documents (in the core document(s) or its annexes), while “supporting documents” (i.e. documents that are not part of the BCR) may only be submitted for reasons of further explanation. Furthermore, it is not necessary to “copy & paste” text from the BCR documents, but it suffices mentioning the relevant sections of the documents as such. Examples: “Section 4.1 of the BCR document and paragraph 2.1 of Annex I (intra-group agreement); Part 2, Section 4 of the Application”, “Section 2.1 of the BCR document and paragraph 3 of Annex 2 (Audit concept)”.

[31] References in this paper to GDPR provisions do not imply that GDPR applies directly to the BCR members acting as data importers, but should rather be understood as the threshold for commitments that need to be made in a BCR. If the BCR make reference to GDPR provisions, possible wording to indicate this might e.g. be “in line with Article X of the GDPR”, “… as those provided for by Article X of the GDPR”.

[32] Please note that, aside from having internal binding nature (i.e. binding effect on the BCR members and their employees), the BCR-P must also have an external binding effect in the sense of providing legal enforceability (of certain parts of the BCR-P) for the data subjects by creating third-party beneficiary rights. See Section 1.3 below as regards this external binding effect.

members, and on their employees				**i. For each BCR member, by one or more of the following:** a) Intra-group agreement; b) Unilateral Declaration (hereinafter “**UD**”), if the following requirements are met: - The entity/entities taking responsibility and liability (see Section 1.4 below) is/are located in a Member State recognising UDs as binding; - The entity/entities taking responsibility and liability (see Section 1.4 below) is/are legally able to bind the other BCR members, and this is expressly provided for, e.g. in a separate written commitment from that entity; - The BCR-P state the principle that all the entities identified in the UD are bound by the BCR-P; - The law applicable to the UD is the law of the country of the entity/entities taking responsibility and liability (see Section 1.4 below). The applicable law is expressly stated in the UD; and - It is the Group’s responsibility to verify that any additional requirements of the applicable law for bindingness are met (such as publication of the UD, …). c) Other means (only if the Group demonstrates how the binding character of the BCR-P is achieved). The BCR Lead can require corresponding documentation that demonstrates the binding character[33].	

[33] The most straightforward instrument in this regard is a contractual arrangement (i.e., an intra-group agreement), since contractual arrangements can be legally enforced by third parties as beneficiaries under private law in all Member States.

				ii. On employees by one or more of: a) Individual and separate agreement(s) / undertaking with sanctions; b) Clause in employment contract with a description of applicable sanctions; c) Collective agreements with sanctions; d) Internal policies with sanctions; or e) Other means. Regarding d) and e) above, the Group should properly demonstrate (1) how those means make the BCR-P legally binding on the employees, and (2) that and that they are enforced in practice vis-à-vis the employees. The BCR Lead can request corresponding documentation that demonstrates the binding character.	
External binding nature and related aspects					
1.3.1 Creation of third-party beneficiary rights that are enforceable by data subjects	YES	YES	Article 47(1)(b), (2)(c) and (e) GDPR	The BCR-P must expressly confer rights to data subjects to enforce the BCR-P as third-party beneficiaries directly against Group members where the requirements at stake are specifically directed to processors in accordance with the GDPR. In this regard, data subjects shall be able to enforce at least the following elements of the BCR-P: • Duty to respect the BCR-P (Section 1.1) • Creation of third-party beneficiary rights that are enforceable by data subjects (Section 1.3.1) • Right to judicial remedies, redress and compensation for data subjects (Section 1.3.3) • One or more BCR member(s) in the EEA with delegated data protection responsibility accept liability for paying compensation to data subjects and	

				remedying breaches of the BCR-P (hereinafter “Liable BCR Member(s)”) (Section 1.4) • The burden of proof lies with the Liable BCR member(s) (Section 1.6) • Easy access to the BCR-P for data subjects (Section 1.7) • Complaint handling process for the BCR-P (Section 3.2) • Duty to cooperate with Competent SAs relating to compliance obligations covered by this third party beneficiary clause (Section 4.1) • Duty to cooperate with the controller and the exporter (Section 4.2) • Obligations to comply with the instructions of the controller (Section 5.1.1) • Purpose limitation (Section 5.1.2) • Accuracy (Section 5.1.3) • Duration of processing and erasure / return of data (Section 5.1.4) • Security of processing (Section 5.1.5) • Sensitive data (Section 5.1.6) • Restrictions on onward transfers to external processors and controllers (Section 5.1.7) • Sub-processing (Section 5.2) • Data subject rights (Section 6) • Local laws and practices affecting compliance with the BCR-P (Section 8.1) • Obligations of the data importer in case of government access requests (Section 8.2) • Termination (Section 9) • Non-Compliance (Section 10)	

				• Duty to inform the data subjects about any update of the BCR-P and of the list of BCR members (Section 11, 4th paragraph) These rights do not extend to those elements of the BCR-P pertaining to internal mechanisms implemented within entities, such as details of training, audit programme, compliance network, and mechanism for updating the BCR-P.[34] The Group needs to make sure that third-party beneficiary rights are effectively created to make those commitments binding, e.g. enforceable by the data subjects. To this aim, the Group needs to provide for and briefly explain in the application form how the instrument(s) that it intends to apply in order to make the BCR-P internally binding (see Section 1.2 above) also enable the data subjects to legally enforce these BCR-P elements against the Group (at least against the member(s) with responsibility and liability as per Section 1.4). For example, if the Group intends to apply an intra-group agreement in this regard (see Section 1.2.i.a), it should briefly explain how such intra group agreement will be enforceable by the data subjects.	
1.3.2 Responsibility toward the controller				The BCR-P should include a statement that the BCR-P will be made binding toward and enforceable for the Controller against any BCR member through a specific reference to them in the processing agreement[35] which shall comply with article 28 of the GDPR. The BCR-P will be annexed to the processing agreement, or a reference to them will be made therein with a possibility of electronic access.	

[34] For reasons of clarity: Those elements are nevertheless subject to possible assessment by the competent SAs and are covered by the Group members' duty to cooperate with the competent SAs (see Section 4.1).

[35] As regards the processing agreement see Chapter 1 ("Introduction"), par. 8.

				Moreover, the BCR-P must state that the Controller shall have the right to enforce the BCR against the BCR member referred to under Section 1.4 in case of a breach of the BCR-P or of the processing agreement by BCR members established outside the EU, or in case of a breach of the written contract referred to under Section 5.2.b ("onward transfers to external sub-processors") by any external sub-processor established outside the EEA.	
1.3.3 Right to judicial remedies, redress and compensation for data subjects	YES	NO	Article 47(2)(e) and Articles 77 to 82 GDPR	The BCR-P shall expressly confer on data subjects the right to judicial remedies and the right to obtain redress and, where appropriate, compensation in case of any breach of one of the enforceable elements of the BCR-P as enumerated in Section 1.3.1 above. The BCR members accept that data subjects may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) GDPR (see Articles 77 – 82 GDPR). The BCR members should make sure that all those rights are covered by the third-party beneficiary clause of the BCR-P, for example, by making reference to the clauses, sections, and/or parts of the BCR-P where those rights are regulated, or by listing them in the said third-party beneficiary clause. The BCR-P must confer on data subjects the right to lodge a complaint (by including a direct reference to such right in the relevant BCR-P documents that are binding and published): - with a SA, in particular in the Member State of the data subject's habitual residence, place of work or place of the alleged infringement; and - before the competent court of the Member States where the controller or processor has an establishment, or where the data subject has their habitual residence.	

				Where the processor and the controller involved in the same processing are found responsible for any damage caused by such processing, the data subject shall be entitled to receive compensation for the entire damage directly from the processor.	
1.4 One or more BCR member(s) in the EEA with delegated data protection responsibility accept liability for paying compensation to data subjects and remedying breaches of the BCR-P (hereinafter "Liable BCR Member(s)")	YES	NO	Article 47(2)(f) GDPR	The BCR-P must contain a duty that, at any given time, one BCR member in the EEA accepts responsibility for and agrees to take the necessary actions to remedy breaches of other BCR members or of external sub-processors established outside of the EEA, and to pay compensation for any material or non-material damages resulting from the violation of the BCR-P by such BCR members or of breaches by external sub-processors established outside of the EEA ("centralised responsibility and liability regime"). SAs may also, on a case-by-case basis, accept solutions where several BCR members established in the EEA have such responsibility and liability, and where sufficient and adequate assurances are provided by the applicant. Where an alternative mechanism to the centralised responsibility and liability regime is used, the applicant should show that data subjects will be transparently informed, assisted in exercising their rights and not disadvantaged or unduly inhibited in any way by the use of such alternative mechanism. The BCR-P should also state that, if a BCR member or an external sub-processor established outside the EEA violates the BCR-P or any sub-processing agreement, the courts or other judicial authorities in the EEA will have jurisdiction, and data subjects will have the rights and remedies against the Liable BCR member as if the violation had been caused by the latter in the Member State in which it is based, instead of the BCR member or the external sub-processor outside the EEA. The Liable BCR member may not rely on a breach by a	

				sub-processor (internal or external of the group) of its obligations in order to avoid its own liabilities.	
1.5 The Liable BCR member(s) has sufficient assets	NO	YES	Article 70(1)(i) GDPR	The application form should confirm that the Liable BCR member(s) has sufficient assets, or has made appropriate arrangements to enable itself to pay compensation for damages resulting from a breach of the BCR-P. Such confirmation should be renewed at the occasion of every annual update (see Section 11 below).	
1.6 The burden of proof lies with the Liable BCR member(s)	YES	NO	Article 47(2)(f) GDPR	The BCR-P must contain the commitment that where data subjects or the controller(s) can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of the BCR-P, it will be for the Liable BCR member to prove that the BCR member outside of the EEA was not responsible for the breach of the BCR-P giving rise to those damages, or that no such breach took place.	
1.7 Easy access to the BCR-P for data subjects	YES	NO	Article 47(2)(g) GDPR	The BCR-P 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. Furthermore, the BCR-P must contain the commitment that data subjects will be provided at least with: • the clause relating to the duty to respect the BCR-P (see Section 1.1) • the third party beneficiary rights that are enforceable by data subjects (see Section 1.3.1), • the clause relating to the responsibility toward the controller (see Section 1.3.2),	

				• the clause relating to the Group’s liability (see Section 1.4 above), • the clause relating to the burden of proof (see Section 1.6) • the clause relating to the duty to provide easy access to the BCR-P for data subjects (see Section 1.7) • the description of the scope of the BCR-P (see Section 2 below), • the description of the complaint handling process (see Section 3.2), • the clause on the duty to cooperate with the competent SA (see Section 4.1), • the clause on the duty to cooperate with the controller and the exporter (see Section 4.2) • the clauses relating to the obligation to comply with the instructions of the Controller (see Section 5.1.1), • the clause relating to purpose limitation (see Sect. 5.1.2), • the clause relating to accuracy (see Section 5.1.3), • the clause relating to the duration of processing and erasure / return of data (see Section 5.1.4), • the clauses relating to security and personal data breach notifications (see Section 5.1.5), • the clause relating to sensitive data (see Section 5.1.6), • the clause relating to restrictions on onward transfers (see Section 5.1.7), • the clause relating to the rights of the data subjects (see Section 6), • the clause on local laws and practices affecting compliance with the BCR-P (see Section 8.1) • the obligations of the data importer in case of government access requests (see Section 8.2)	

				This information should be up-to-date, and presented to data subjects in a clear, intelligible, and transparent way.[36] This information should be provided in full, hence a summary hereof will not be sufficient. Moreover, the BCR-P must illustrate the way in which such information will be provided. For instance, the BCR-P may state that at least the parts of the BCR-P on which information to data subjects is mandatory (as described in the previous paragraphs) will be published on the internet or on the intranet (when data subjects are only the Group staff having access to the intranet). In case the Group plans to not publish the BCR-P as a whole, but only certain parts or a specific version aimed at informing data subjects, the Group should expressly provide in the BCR-P the list of the elements that it will include in that public version. In such situation, the description of the material scope of the BCR-P[37] should always be part of the information on the BCR-P that is publicly available. The list of definitions (see Section 12 below) and, if applicable, of abbreviations which are used in the BCR-P, should in any case be included in the parts of the BCR-P which are published. The BCR-P should contain an express commitment in this regard. The BCR-P must use clear and plain language so that employees and any other person in charge with applying the BCR-P can sufficiently understand them. The same applies to any parts/version of the BCR-P that will be published with the aim of providing access to the BCR-P for data subjects.	

[36] See Guidelines on Transparency under Regulation 2016/679, WP260rev.01, endorsed by the European Data Protection Board on 25/05/2018.

[37] See Section 2.1 below.

2 - SCOPE OF THE BCR					
2.1 Description of the material scope of the BCR-P	YES	YES	Article 47(2)(b) GDPR	In order to be transparent as to the scope of the BCR-P, the BCR-P must provide a description of the material scope, i.e. of envisaged transfers that may be carried out on the basis of the BCR-P. These transfers should be described as precisely as possible in the BCR-P.[38] The BCR-P must, in particular, specify per transfer or set of transfers[39] (e.g., by means of a table): - the categories of personal data; - the type of processing and their purposes; - the categories of data subjects (e.g. data related to employees, contractors, clients, customers, suppliers, service providers and other third parties as part of the Group's respective regular business activities); and - the third country or countries. As to the data subjects covered, BCR-P will apply to all data subjects whose personal data are transferred within the scope of the BCR-P from an entity under the scope of application of Chapter V GDPR. Therefore, the scope of the BCR-P may, in particular, not be limited to "EEA citizens or EEA residents".	

[38] Please note that, while the BCR-P only need to include a general description of the envisaged transfers that may be carried out under the BCR-P, this does not limit the controller's, the processor's and any sub-processor's obligations to describe in each processing agreement and any subprocessing agreement (at least in the instructions given to the processor(s) and passed on to each subprocessor) the covered processing activities with the degree of specificity as mandatorily required by Article 28(3) and (4) GDPR (subject-matter and duration of processing, nature and purpose of the processing, type of personal dasta, categories of data subjects). This may therefore require adding to the description of the transfers as given in the BCR-P more detailed descriptions in each controller - processor and each processor - sub-processor relationship, i.e. either in the processing agreement(s) and the sub-processing agreement(s) or at least in the instructions given to the processor(s) and passed on to each subprocessor.

[39] The information on the transfers must be exhaustive in that every envisaged transfer or set of transfers must be described. This does not mean that the information must be provided with a high degree of specificity or granularity. Where the description provided by the applicant is too broad, general or vague, the applicant should be able to explain why it is not in a position to provide more detailed information. If and to the extent that any of the elements provided in the transfers' description changes in the future, the process for BCR-P updates applies, i.e., information on the amendments to the BCR-P must be provided in the annual BCR-P update notified to the BCR Lead (see Section XX below). See also the previous footnote.

2.2 List of BCR members, and description of the geographical scope of the BCR-P	YES	YES	Article 47(2)(a) GDPR	The BCR-P 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-P, for example an annex thereof, that has to be published along with the BCR-P).[40] The BCR-P should indicate that they at least apply to all personal data processed by members of the Group covered by the geographical scope of the GDPR acting as processors on behalf of controllers that are not members of the Group and which are then transferred by such processors to BCR members outside the EEA, including any onward transfers to other BCR members outside the EEA.	
3 - EFFECTIVENESS					
3.1 Suitable training programme	YES	YES	Article 47(2)(n) GDPR	The BCR-P must state that appropriate and up-to-date training on the BCR-P is provided to personnel that have permanent or regular access to personal data, who are involved in the collection of data or in the development of tools used to process personal data. The training programme, including its materials, has to be developed to a sufficiently elaborate degree before the BCR-P are approved. In this regard it should be recalled that no transfer can be made under the BCR-P to a BCR member unless the member is effectively bound by the BCR-P and can deliver compliance (see Section 7.1) which includes that appropriate training on the BCR-P can effectively be provided to the employees of the respective member.	

[40] Please note that notwithstanding the list, according to Article 28(2) GDPR the processor requires the controller's prior authorization for engaging any sub-processor, even if included in the list. Moreover, the BCR-P must also include an obligation for group members not to engage both internal and external processors unless there is a prior specific or general written authorisation by the controller (see Section 5.2).

				Training intervals should be specified in the BCR-P. Training should cover, among others, procedures of managing requests for access to personal data by public authorities. The SAs evaluating the BCR-P may ask for examples and explanations of the training programme during the application procedure.	
3.2 Complaint handling process for the BCR-P	YES	NO	Article 47(2)(i) and Article 12(3) GDPR	All BCR members shall have the duty to communicate any claim or request related to compliance by any group member with the BCR-P, and also any claim or request related to controller and/or processor and/or sub-processor obligations with regards to the processing covered by the processing agreement or the sub-processing agreement, without undue delay to the controller without obligation to handle it, except if it has been agreed otherwise with the Controller. An internal complaint handling process must be set up in the BCR-P to ensure that any data subject should be able to exercise their rights and complain about any BCR member. The BCR-P (or the parts of the BCR-P that will be published for the attention of data subjects, see Section 1.7) 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-P. 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. web forms, a generic e-mail address and/or a phone number. While data subjects are encouraged to use the point(s) of contact indicated, this is not mandatory. The BCR-P must contain the duty for the group members to provide information on actions taken to the complainant	

				without undue delay, and in any event within one month, by a clearly identified department or person with an appropriate level of independence in the exercise of their functions. Taking into account the complexity and number of the requests, that one-month period may be extended at maximum by two further months, in which case the complainant should be informed accordingly. The BCR-P should in any case include the following information about the complaint process: - Where to complain (point(s) of contact; see above); - In what form; - Consequences of delays for the reply to the complaint; - Consequences in case of rejection of the complaint; - Consequences in case the complaint is considered as justified; and Consequences if the data subject is not satisfied by the reply, i.e., right to lodge a claim before the competent court and a complaint before a SA (see Section 1.3.2 above), while clarifying that such right is not dependent on the data subject having used the complaint handling process beforehand.	
3.3.1 Audit programme covering the BCR-P	YES	NO	Article 47(2)(j) and (l), and Article 38(3) GDPR	The BCR-P must create a duty for the Group to have data protection audits on a regular basis (by either internal and/or external accredited auditors) and if there are indications of non-compliance to ensure verification of compliance with the BCR-P. The audit frequency envisaged should be specified in the BCR-P. The frequency needs to be determined on the basis of the risk(s) posed by the processing activities covered by the BCR-P to the rights and freedoms of data subjects.	

				In addition to the regular audits, specific audits (ad hoc audits) may be requested by the Privacy officer or Function (see Section 3.4 below), or any other competent function in the organisation. If audits will be carried out by external auditors[41], the BCR-P should specify the conditions under which such auditors are entrusted. The BCR-P should state which actor (department within the Group) decides on the audit plan/programme, and which actor will conduct the audit. Data protection officers should not be the ones in charge of auditing compliance with the BCR-P, if such situation can result in a conflict of interests.[42] 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-P include an explicit commitment in this regard. The BCR-P should state that the audit plan covers all aspects of the BCR-P (i.e. applications, IT systems, databases that process personal data, or onward transfers, decisions taken as regards mandatory requirements under national laws that conflict with the BCR-P, review of the contractual terms used for the transfers out of the Group, corrective actions, etc.), including methods and action plans ensuring that corrective actions have been implemented. It is not mandatory to monitor all aspects of the BCR-P each time a BCR member is audited, as long as all aspects of the	

[41] As regards the qualifications of external auditors, see Sect. 3.3.2
[42] See WP243 rev01, p. XXX

				BCR-P are monitored at appropriate regular intervals for that BCR member. Moreover, the BCR-P should state that the results will be communicated: - to the Privacy officer or Function (see Section 3.4 below); - to the board of the Liable BCR member; and - where appropriate, also to the Group's ultimate parent's board - to the controller. The BCR-P must state that Competent SAs shall have access to the results of the audit upon request.[43]	
3.3.2 Audit by the controller and the exporter	YES	YES	Art. 28(3)(h)	Any member of the Group processing the personal data on behalf of a controller will accept, at the request of that controller, at reasonable intervals or if there are indications of non-compliance, to submit their data processing facilities for audit by the controller of the processing activities relating to that controller, or by another independent auditor mandated by the controller. Audits can also be carried out by the exporter or an independent auditor selected by the exporter. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.	
3.4 Creation of a network of data protection officers (DPOs) or appropriate staff	YES	YES	Article 47(2)(h) and Article 38(3) GDPR	The BCR-P must contain a commitment to designate a DPO, where required in line with Article 37 GDPR, or any another designated privacy professional (such as a chief privacy officer) with the responsibility to monitor compliance with the	

[43] Since SAs are already bound by an obligation of confidentiality in the course of exercising their public office (see in particular Article 54(2) GDPR), the BCR-P should not contain wording aimed at restricting the duty of all BCR members to communicate the results of the audit(s) to the SAs on grounds of confidentiality, e.g. related to the protection of business secrets.

for monitoring compliance with the BCR-P				BCR-P, who enjoys the support of the highest management to fulfil this task. The DPO or the other designated privacy professional can be assisted by a team, a network of local DPOs or local contacts, as appropriate (hereinafter “**Privacy officer or Function**”). The DPO shall directly report to the highest management level. In addition, the DPO must be able to inform the highest management level if any questions or problems arise during the performance of their duties. The BCR-P shall include a brief description of the internal structure, role, position and tasks of the DPO or similar function and the network created to ensure compliance with the BCR-P. For example, that the DPO or chief privacy officer informs and advises the highest management, deals with Competent SAs’ investigations, monitors and annually reports on compliance at a global level, and that local DPOs or local contacts can be in charge of handling local complaints from data subjects, reporting major privacy issues to the DPO, monitoring training and compliance at a local level. The DPO should not have any tasks that could result in conflict of interests. 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-P 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. The BCR-P should specify that the DPO or other privacy professionals may be directly contacted. The BCR-P should include a commitment to publish their contact details.	

4 - COOPERATION DUTY					
4.1 Duty to cooperate with Competent SAs	YES	NO	Article 47(2)(l) GDPR and Article 31 GDPR	The BCR-P should contain a clear duty for all BCR members: to cooperate with, to accept to be audited and to be inspected, including where necessary, on-site, by the competent SAs, - to take into account their advice, and - to abide by decisions of these SAs on any issue related to the BCR-P. The BCR-P shall include the obligation to provide the Competent SAs, upon request, with any information about the processing operations covered by the BCR-P. Since SAs are already bound by an obligation of confidentiality in the course of exercising their public office[44] (see in particular Article 54(2) GDPR), the BCR-P may not contain wording aimed at restricting the duty of all BCR members to cooperate with the Competent SAs, to take into account their advice, to abide by their decisions or to accept to be audited and to be inspected by them including, where necessary, on-site, or to accept audits by them on grounds of confidentiality, e.g. related to the protection of business secrets. The BCR-P cannot limit the duty to cooperate with Competent SAs nor limit their powers, in particular in relation to the practical modalities of the audits conducted by these SAs (e.g., not limited to business hours). The BCR-P need to include a commitment that any dispute related to the Competent SAs' exercise of supervision of compliance with the BCR-P will be resolved by the courts of	

[44] see in particular Article 54(2) GDPR

				the Member State of that SA, in accordance with that Member State’s procedural law. The BCR members agree to submit themselves to the jurisdiction of these courts.	
4.2 Duty to cooperate with the controller and the exporter	YES	NO		Group members will have a duty to cooperate with and to promptly make available to the controller all information necessary to allow the controller to comply with its obligations under data protection law and all information necessary to demonstrate compliance with their obligations under the BCR and the processing and/or the sub-processing agreement. Group members that act as data importers will also have a duty to promptly make available such information to the Group member acting as data exporter at the data exporter’s request or on instructions of the controller.	
5 - DATA PROTECTION SAFEGUARDS					
5.1.1 Obligation to comply with the instructions of the Controller	YES	NO	Article 28(3) GDPR)	The BCR-P shall explicitly include and describe the following obligations to be observed by the BCR members, which should be drafted in a sufficiently elaborated manner that is in line with the content of these obligations as provided for in the GDPR provisions: - The data exporter[45] shall inform, prior to making the data available to the data importer, the data importer that it acts as processor under the instructions of the controller(s), and the documented instructions of the controller will be made available to the importer prior to the processing; - The data importer shall process the personal data only on documented instructions from the controller as communicated to the data importer by the data exporter, and any additional instructions from the data exporter (which should not conflict with the instructions from the controller). The controller or data exporter may give further documented	

[45] Throughout this paper, „data exporter“ is the BCR-P member that transfers personal data as processor under the instructions of the controller according to Article 28(3)(a) GDPR.

				instructions regarding the data processing throughout the duration of the contract; - The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller; In addition, Group members shall immediately inform the controller if in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. - The data exporter shall assure that the same data protection obligations are imposed on the data importer as set out in the processing agreement entered into between the controller and the data exporter.	
5.1.2 Purpose limitation	YES	NO		BCR Group members acting as importers[46] should process the personal data only for the specific, explicit and legitimate purpose(s) of the transfer, as set out in the processing agreement, unless on further instructions from the controller, as communicated to the data importer by the data exporter.	
5.1.3 Accuracy	YES	NO		BCR Group members acting as data importers[47] should inform the data exporter without undue delay if they become aware that the personal data it has received is inaccurate, or has become outdated; in this case, the data importer, together with the data exporter, shall cooperate with the controller to rectify or erase the data in order for the controller to fulfill its obligations under data protection law.	
5.1.4 Duration of processing and erasure / return of data	YES	NO		Processing by the data importer shall only take place for the duration specified in the sub-processing agreement.[48] After the end of the provision of the processing services, the data	

[46] In case the BCR-P are used as a Global Policy (see Introduction, Par. 14), this obligation should not be limited to Group members acting as importers.

[47] See footnote 44.

[48] See footnote 40.

				importer shall, in accordance with the instructions of the controller, as communicated to the data importer by the data exporter, delete all personal data processed on behalf of the controller and demonstrate to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with the obligations stemming from the BCR. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with the BCR or – if the BCR ceased to exist – with the same level of protection as provided for by the BCR, and will only process it to the extent and for as long as required under that local law. This is without prejudice to Section 8, in particular the requirement for the data importer to notify the data exporter if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Section 8.	
5.1.5 Security of processing	YES	NO		(a) The data importer and also the data exporter shall implement appropriate technical and organisational measures to ensure, the **security** of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that personal data (hereinafter ‘personal data breach’) including during the transmission by the data exporter to the data importer. In assessing the appropriate level of security, due account shall be taken of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose(s) of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for	

				attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the controller or, if applicable, with a trusted third party (hereinafter TTP)[49] which shall only act on written instruction and/or authorization by the controller.[50] In complying with its obligations under this paragraph, the data importer shall implement technical and organisational measures as agreed on with the controller in the processing agreement or as required by way of documented instructions provided by the controller. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security. (b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the agreement. It shall ensure that persons authorised to process the personal data have committed themselves to **confidentiality** or are under an appropriate statutory obligation of confidentiality. (c) In the event of **a personal data breach** concerning personal data processed by the data importer under the BCR, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and	

[49] A person or body, not being the Controller or Exporter, that, in case of pseudonomised data, is in charge and responsible of holding the key in order to safeguard the privacy of natural persons (i.e. data subject under the meaning of art. 4(1) GDPR). The trusted third party acts in an independent manner and ensures that the re-identification key is not disclosed to anyone that is not authorised by the Controller to access the personal data.

[50] The Controller shall provide written instructions to the TTP in the Service Level Agreement and/ or other legal act under Union or Member State law that is binding on the TTP with regards to the Controller, that sets out the conditions to access the identification key.

				approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information available and further information shall, as it becomes available, subsequently be provided without undue delay. (d) In the event of a personal data breach the data importer shall cooperate with and **assist the data exporter** to enable the data exporter to comply with its obligations under EEA data protection law , in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.	
5.1.6 Sensitive Data	YES	NO		Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards as instructed by the controller in the processing agreement or as required by way of documented instructions provided by the controller.	
5.1.7 Restrictions on onward transfers to external processors and controllers	YES	NO	Article 47(2)(d) GDPR and Article 44 GDPR	The data importer shall only disclose the personal data to an external third party (controller or processor) on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to an external third party (controller or	

				processor) located outside the EEA (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if • the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 GDPR that covers the onward transfer; • the third party ensures appropriate safeguards pursuant to Articles 46 or 47 GDPR and is able to comply with all commitments; or in the absence of an adequacy decision or appropriate safeguards, BCR-P may include a provision that onward transfers may exceptionally take place if a derogation applies in line with Article 49 GDPR.	
5.2 Sub-processing	YES	NO		(a) Members of the Group acting as importers may not engage any **internal or external**[51] subprocessors without prior specific or general written authorisation of the controller; the processing agreement will specify if a general prior authorization given at the beginning of the service would be sufficient or if a specific authorization will be required for each new subprocessor. If a general authorization is given, the controller should be informed by the importer of any intended changes concerning the addition or replacement of a subprocessor in such a timely fashion that the controller has the possibility to object to the change or to terminate the contract before the data are communicated to the new subprocessor. In any case, also the exporter should be informed by the importer of the engagement of subprocesssors.	

[51] See Footnotes 6 and 7 for the definitions of “internal”/”external” (controller/processor/subprocessor).

				(b) Where a data importer engages an external sub-processor[52] to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations (including in terms of third-party beneficiary rights for data subjects) as those binding the importer under the sub-processing agreement entered into with the exporter, and under Sections 1.3, 3.3.2, 4.1, 4.2, 5, 6, 8.1 and 8.2 of the BCR-P. Group members acting as data exporters and data importers agree that, by complying with this clause, the data importer also fulfils its obligations under Section 5.1.7. The data importer shall ensure that the external subprocessor complies with the obligations to which the data importer is subject pursuant to this clause 5.2(b). (c) The data importer shall provide, at the data exporter's or the controller's request, a copy of such written contract and any subsequent amendments. (d) The data importer shall remain fully responsible to the data exporter and the controller for the performance of the subprocessor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor to fulfil its obligations under that contract. (e) The data importer shall agree a third-party beneficiary clause with the subprocessor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter, as instructed by the controller, shall have the right to terminate the	

[52] Please recall that Group members enlisted as ("internal") sub-processors by Group members acting as importers are already bound by the BCR-P (see par. 6 of the Introduction), while external sub-processors are not. Instructions issued by the controller shall in any case be passed on by importers to both internal and external sub-processors.

				subprocessor contract and to instruct the subprocessor to erase or return the personal data.	
6. DATA SUBJECT RIGHTS					
				(a) Any BCR member acting as data importer[53] shall promptly notify the data exporter and, where instructed to do so by the controller or at the controller's order as communicated by the exporter, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller or, at the controller's instruction, by the exporter. (b) Group members acting as data importers shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under the GDPR.[54] (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.	
7. TOOLS FOR COMPLIANCE					
	YES	NO	Article 47(2)(d), and Articles 30, 35-36 GDPR	The BCR-P should contain a commitment that, in order to demonstrate compliance, BCR members have to maintain a **record of all categories of processing activities** carried out on behalf of each controller on personal data transferred under these BCR-P. The BCR-P must specify the content of the record, in line with what is required by Article 30(2) (for processors). This record should be maintained in writing,	

[53] See footnote 48.

[54] In this regard, each exporter and importer shall set out, for each transfer or set of transfers, the appropriate technical and organisational measures to be taken by the data importer to be able to provide assistance to the controller and the exporter. This could be e.g. done in one or several Annexes entered into by the respective exporter(s) and importer(s) aside from the BCR-P and which should be linked to the BCR-P through a reference. The technical and organisational measures are not integral part of the BCR and will not be verified in the approval procedure.

				including in electronic form, and should be made available to the Competent SA on request. The BCR-P should contain the commitment that the BCR members will assist the controller with **data protection impact assessments** to be carried out for processing operations on personal data transferred under these BCR-P that are likely to result in a high risk to the rights and freedoms of natural persons[55].	
8. LOCAL LAWS AND GOVERNMENT ACCESS REQUESTS					
8.1 Local laws and practices affecting compliance with the BCR-P[56]	YES	NO	Article 47(2)(m) GDPR	The BCR-P shall contain a clear commitment that BCR members will use the BCR-P as a tool for transfers only where they have assessed, in agreement with the controller, 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 the data importer from fulfilling its obligations under these BCR-P. The BCR-P should further specify that this is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society[57] to safeguard one of the objectives listed in Article 23(1) GDPR, and are not in contradiction with the BCR-P. The BCR-P should also contain a commitment that, in assessing the laws and practices of the third country which may affect the respect of the commitments contained in the	

[55] See Article 35 GDPR

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

[57] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

				BCR-P, the BCR members have taken due account, in particular, of the following elements: i. The specific circumstances of the transfers or set of transfers, and of any envisaged onward transfers within the same third country or to another third country, including: - purposes for which the data are transferred and processed (e.g. marketing, HR, storage, IT support, clinical trials); - types of entities involved in the processing (the data importer and any further recipient of any onward transfer); - economic sector in which the transfer or set of transfers occur; - categories and format of the personal data transferred; - location of the processing, including storage; and - transmission channels used. ii. The laws and practices of the third country of destination that are relevant in light of the circumstances of the transfer[58], including those requiring to disclose data to public authorities or authorising access by such authorities and those providing for access to these data during the transit between the country of the data exporter and the	

[58] As regards the assessment of the impact of the laws and practices of the third countries, please see EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

				country of the data importer, as well as the applicable limitations and safeguards[59]. iii. Any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the BCR-P, including measures applied during the transmission and to the processing of the personal data in the country of destination. The BCR-P should also contain a commitment that where any safeguards in addition to those envisaged under the BCR-P should be put in place, the Liable BCR member(s), and the relevant Privacy officer or Function will be informed and involved in such assessment.[60] The BCR-P should contain also an obligation for the BCR members to document such assessment, as well as the supplementary measures selected and implemented. They should make such documentation available to the competent SAs and to the controller upon request. The BCR-P should oblige any BCR member acting as data importer to promptly notify the data exporter if, when using these BCR-P as a tool for transfers, and for the duration of the BCR membership, it has reasons to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the BCR-P, including following a change in the laws in the third country or a measure (such as a disclosure request). This information	

[59] With regards to the impact of such laws and practices on compliance with the BCR-P, 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 time-frame. 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 the BCR, it needs to be supported by other relevant, objective elements, and it is for the BCR members to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the BCR members 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.

[60] It should be noted that the relevant controller on behalf of which the transfer of the personal data is carried out has the responsibility to verify the assessment (see also Introduction, Par. 13).

				should also be provided to the Liable BCR member(s) and to the controller. Upon verification of such notification, the BCR member acting as data exporter, along with the Liable BCR member(s) and the relevant Privacy officer or Function, should commit to promptly identify supplementary measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the BCR member acting as data exporter and/or data importer, in agreement with the controller, in order to enable them to fulfil their obligations under the BCR-P. The same applies if a BCR member acting as data exporter has reasons to believe that a BCR member acting as its data importer can no longer fulfil its obligations under this BCR-P. Where the BCR member acting as data exporter, along with the Liable BCR member(s) and the relevant Privacy officer or Function, assesses that the BCR-P – even if accompanied by supplementary measures – cannot be complied with for a transfer or set of transfers, or if instructed by the controller or the competent supervisory authorities, it must suspend the transfer or set of transfers at stake, as well as all transfers for which the same assessment and reasoning would lead to a similar result, until compliance is ensured or the transfer is ended. The BCR-P must contain a commitment that following such a suspension, the BCR member acting as data exporter, in agreement with the controller, has to end the transfer or set of transfers if the BCR-P cannot be complied with and compliance with the BCR is not restored within one month of suspension. In this case, personal data that have been transferred prior to the suspension, and any copies thereof, should, at the choice of the controller, be returned to it or destroyed in their entirety.	

				The BCR-P should contain a commitment that the Liable BCR member(s) and the relevant Privacy officer or Function will inform all other BCR members of the assessment carried out and of its results, so that the identified supplementary measures will be applied, in agreement with the controller, in case the same type of transfers is carried out by any other BCR member or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended. The BCR-P should include a duty for data exporters to monitor, on an ongoing basis, and where appropriate in collaboration with data importers, developments in the third countries to which the data exporters have transferred personal data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers, and to inform the controller in case they identify such developments.	
8.2 Obligations of the data importer in case of government access requests	YES	NO	Article 47(2)(m) GDPR	Without prejudice to the obligation of the BCR member acting as data importer to inform the data exporter and the controller of its inability to comply with the commitments contained in the BCR-P (see Section 8.1 above), the BCR-P should in any case include the following commitments: i. The BCR member acting as data importer will promptly notify the data exporter and the controller and, where possible, the data subject (if necessary with the help of the data exporter) if it: a) receives a legally binding request by a public authority under the laws of the country of destination, or of another third country, for disclosure of personal data transferred pursuant to the BCR-P; such notification will include information about the personal data requested, the requesting	

				authority, the legal basis for the request and the response provided; b) becomes aware of any direct access by public authorities to personal data transferred pursuant to the BCR-P in accordance with the laws of the country of destination; such notification will include all information available to the data importer. ii. If prohibited from notifying the data exporter and/or the controller and/or the data subject, the data importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the data exporter. iii. The data importer will provide the BCR member acting as data exporter and the controller, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the data importer is or becomes partially or completely prohibited from providing the data exporter with the aforementioned information, it will, without undue delay, inform the data exporter accordingly. 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-P, and shall make it available to the Competent SAs upon request. v. The data importer will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority,	

				and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and principles of international comity. The data importer will, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the personal data requested until required to do so under the applicable procedural rules. vi. The data importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter and the controller. It will also make it available to the Competent SAs upon request. vii. The data importer will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. In any case, the BCR-P should state that transfers of personal data by a BCR member to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary and proportionate in a democratic society[61] (as to the consequences of such cases, see Section 5.4.1 above).	

[61] See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

9- TERMINATION					
	YES	NO	Article 70(1)(i) GDPR	The BCR-P should specify that a data importer which ceases to be bound by the BCR-P should, at the choice of the controller, delete or return all personal data processed on behalf of the controller, delete existing copies and demonstrate it has done so. If, pursuant to the controller's choice, the data are kept by the importer, the importer should inform the controller and guarantee the confidentiality of data and that it will not actively process the data transferred anymore. This is without prejudice to any requirements under third country law applicable to the data importer prohibiting return or destruction of the personal data. In that case, the data importer should guarantee to apply the same level of protection granted by the BCR-P and to process the data only for as long as required under that third country law.	
10 – NON-COMPLIANCE					
	YES	NO	Article 70(1)(i) GDPR	The BCR-P should contain commitments as to the following obligations: i. No transfer is made to a BCR member unless the BCR member is effectively bound by the BCR-P. ii. The data importer should promptly inform the data exporter and the controller if it is unable to comply with the BCR-P, for whatever reason, including the situations further described under Section 8.1 above. iii. Where the data importer is in breach of the BCR-P or unable to comply with them, the data exporter should suspend the transfer.	

				iv. The data importer should, at the choice of the data controller, immediately return or delete the personal data that has been transferred under the BCR-P in its entirety, where: - the data exporter has suspended the transfer, and compliance with this BCR-P is not restored within a reasonable time, and in any event within one month of suspension; or - the data importer is in substantial or persistent breach of the BCR-P; or - the data importer fails to comply with a binding decision of a competent court or Competent SA regarding its obligations under the BCR-P. The same commitments should apply to any copies of the data. The data importer should certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer should continue to ensure compliance with the BCR-P. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer should warrant that it will continue to ensure compliance with the BCR-P, and will only process the data to the extent and for as long as required under that local law. For cases were applicable local laws and/or practices affect compliance with the BCR-P, see Section 8.1 above.	

11 - MECHANISMS FOR REPORTING AND RECORDING CHANGES: Process for updating the BCR-P					
	YES	NO	Article 47(2)(k) GDPR	The BCR-P should be kept up-to-date in order to reflect the current situation (e.g., to take into account modifications of the regulatory environment, these EDPB Recommendations, or changes to the scope of the BCR-P). The BCR-P should impose a duty to report changes, including to the list of BCR members, without undue delay, **to all BCR members and to the controller**. Where a change affects the processing conditions, the information should be given to the controller in such a timely fashion that the controller has the possibility to object to the change or to terminate the contract before the modification is made (e.g., on any intended changes concerning the addition or replacement of subcontractors, before the data are communicated to the new sub-processor). The BCR-P should identify a person or team/department that keeps a fully updated list of the BCR members, keeps record of any updates to the BCR-P, and provides the necessary information **to data subjects,** and, upon request, **to Competent SAs and the controller**. Where a modification to the BCR-P would possibly be detrimental to the level of the protection offered by the BCR-P 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. Once a year, the SAs should be notified via the BCR Lead of any changes to the BCR-P or to the list of BCR members, with the brief explanation of the reasons for the changes. This	

				includes any changes made in order to align the BCR-P with any updated version of these EDPB recommendations. The SAs should also be notified once a year in instances where no changes have been made. The annual update or notification should also include the renewal of the confirmation regarding assets (see Section 1.5 above). It remains the responsibility of the BCR-P holder to keep it up-to-date and in compliance with Article 47 GDPR and these EDPB Recommendations.	
12 - DEFINITIONS					
	YES	NO	Article 70(1)(i) GDPR	The applicant should include a list of definitions in the BCR-P. The list should include the most relevant terms. To the extent the BCR-P contain terms defined in the GDPR, the definitions provided should not vary from the GDPR. For readability, these definitions should be replicated in the list. If the terms “data exporter” and “data importer” are used, they must be defined. The applicant may find it useful to add further terms and their definitions. If the term “Competent SA(s)” is used, it should be defined as referring to both the EEA data protection SA competent for the data exporter and the data protection SA competent for the controller.[62] Where the term “applicable law” is used, it should be clarified, in each case, whether it refers to national/local law of a third country as applicable to the BCR members. In any case, BCR members must comply with the requirements set out under Sections 8.1 and 8.2 above. References to GDPR provisions should generally be avoided. However, if there is a need for reference to a particular	

[62] See also Introduction, paragraph 11.

				provision of the GDPR, it should be quoted in full in the BCR-P.	

For the European Data Protection Board

The Chair

(Anu Talus)