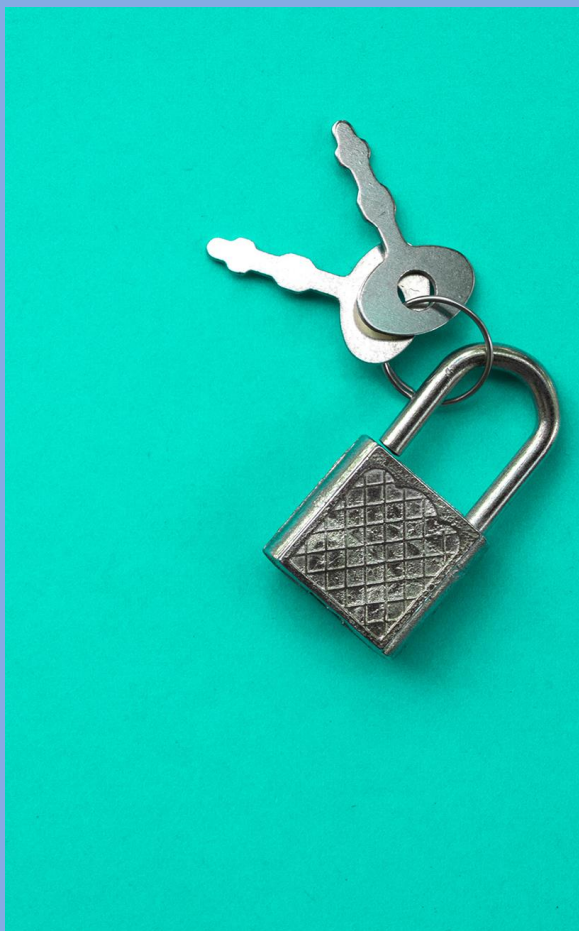
Bird & Bird

Latest Updates to EU BCRs

Version 2

July 2023



EUROPEAN DATA PROTECTION BOARD

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)

The recommendations will be subject to public consultation until 10 January 2023.

ELEMENTS AND PRINCIPLES TO BE FOUND IN BCR-C

Criteria for BCR-C approval	In BCR-C	In application form	Reference	Comments	References to BCR-C, application form BCR-C, and / or supporting documents[1]
1 - BINDING NATURE					
INTERNALLY					
1.1 Duty to respect the BCR-C	YES	NO	Article 47(1)(a) and (2)(c) GDPR[2]	The BCR-C must be legally binding and should contain a clear duty for each BCR member, including their employees, to respect the BCR-C.	
1.2 1.2 Explanation of how the BCR-C are internally[3] made	NO	YES	Article 47(1)(a) and (2)(c) GDPR	The Group will have to explain in its application form how the BCR-C are made binding: i. For each BCR member, by one or more of the following:	

[1] 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)".

[2] 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".

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

binding on the BCR members, and on their employees				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-C state the principle that all the entities identified in the UD are bound by the BCR-C; - 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-C is achieved). The BCR Lead can require corresponding documentation that demonstrates the binding character.[4] 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;	

[4] 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.

				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-C legally binding on the employees, and (2) that and how they will be enforced in practice vis-à-vis the employees. The BCR Lead can request corresponding documentation that demonstrates the binding character.	
EXTERNALLY					
1.3.1 Creation of third-party beneficiary rights that are enforceable by data subjects~~. Including the possibility to lodge a complaint before the competent SA and before the courts~~	YES	~~YES~~ ~~NO~~YES	Article 47(1)(b), (2)(c) and (e) GDPR	The BCR-C must expressly confer rights to data subjects to enforce the BCR-C as third-party beneficiaries, at least as regards the following elements of the BCR-C: - Data protection principles, lawfulness of processing, security and personal data breach notifications, restrictions on onward transfers (see Article 47(2)(d) GDPR, and Sections 5.1.1, 5.1.2, 5.1.3 second paragraph 3rd indent ["duty to notify without undue delay to data subjects where the personal data breach is likely to result in a high risk to their rights and freedoms"], and 5.1.4 below); - Transparency and easy access to the BCR-C (see Article 47(2)(g) GDPR, and Sections 1.7 and 5.1.1 below); - Rights of information, access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling (see Article 47(2)(e), Articles 15 to 19, 21 and 22 GDPR, and Section 5.2 below);	

				~~- National legislation preventing respect of BCRs (Art. 47.2.m and Section 6.3 of this referential),~~ - Obligations in case of local laws and practices affecting compliance with the BCR-C and in case of government access requests (see Article 47(2)(m) GDPR, and Section 5.4.1 and 5.4.2 below); - Right to complain through the Group's internal complaint process (see Article 47(1)(i) GDPR, and Section 3.2 below); - Cooperation duties with Competent SAs (see Article 47(2)(j), (k), and (l) GDPR, and Section 4.1 below) relating to compliance obligations covered by this third party beneficiary clause; - Jurisdiction and liability provisions (see Article 47(2)(e) and (f) GDPR, and Sections 1.3.2 and 1.4 below); - Duty to inform the data subjects about any update of the BCR-C and of the list of BCR members, e.g. by way of publishing the new version without delay (see Section 8.1 below); - Third-party beneficiary clause itself (see present Section 1.3.1); - Right to judicial remedies, redress and compensation (see Section 1.3.2 below) These rights do not extend to those elements of the BCR-C pertaining to internal mechanisms implemented within entities, such as details of training, audit programme, compliance network, and mechanism for updating the BCR-C. 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 (see Section 1.2 [~~below~~above]).	

				To this aim, the Group needs to provide for and briefly explain in the application form how the instrument(s) it intends to apply in order to make the BCR-C internally binding (see Section 1.2 above) also enable the data subjects to legally enforce these BCR-C 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 Right to judicial remedies, redress and compensation for data subjects	YES	NO	Article 47(2)(e) and Articles 77 to 82 GDPR	The BCR-C 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-C 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-C must confer on data subjects the right to lodge a complaint (by including a direct reference to such right in the relevant BCR-C 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.	

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-C (hereinafter "Liable BCR Member(s)")	YES	~~YES~~ NO	Article 47(2)(f) GDPR	The BCR-C 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 the acts of other BCR members outside of the EEA, and to pay compensation for any material or non-material damages resulting from the violation of the BCR-C by such BCR members ("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-C should also state that, if a BCR member outside the EEA violates the BCR-C, 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 outside the EEA.	
1.5 The Liable BCR member(s) has sufficient assets	NO	YES	Article 70(1)(i) GDPR	The application form should contain a confirmation 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-C. Such confirmation should be renewed at the occasion of every annual update (see Section 8.1 below).	

1.6 The burden of proof lies with the Liable BCR member(s)	YES	~~YES~~ NO	Article 47(2)(f) GDPR	The BCR-C must contain the commitment that where data subjects 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-C, 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-C giving rise to those damages, or that no such breach took place.	
1.7 Easy access to the BCR-C for data subjects	YES	NO	Article 47(2)(g) GDPR	The BCR-C must contain the commitment that all data subjects should be provided with ~~the information as required by Articles 13 and 14 GDPR,~~ 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-C must contain the commitment that data subjects will be provided at least with the description of the scope of the BCR-C (see Section 2 below), the clause relating to the Group's liability (see Section 1.4 above), the clauses relating to the data protection principles (see Section 5.1.1 below), to the lawfulness of the processing (see Section 5.1.2 below), to security and personal data breach notifications (see Section 5.1.3 below), to restrictions on onward transfers (see Section 5.1.4 below), and the clauses relating to the ~~data protection principles~~rights of the data subjects (see Section 5.2 below). This information should be up-to-date, and presented to data subjects in a clear, intelligible, and transparent way[5]. This information should be provided in full, hence a summary hereof will not be sufficient. Moreover, the BCR-C must illustrate the way in which such information will be provided. For instance, the BCR-C may state that at least the parts of the BCR-C on which	

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

				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-C as a whole, but only certain parts or a specific version aimed at informing data subjects, the Group should expressly provide in the BCR-C the list of the elements that it will include in that public version. In such situation, the description of the material scope of the BCR-C[6] should always be part of the information on the BCR-C that is publicly available. The list of definitions (see Section 9.1 below) and, if applicable, of abbreviations which are used in the BCR-C, should in any case be included in the parts of the BCR-C which are published. The BCR-C should contain an express commitment in this regard. The BCR-C must use clear and plain language so that employees and any other person in charge with applying the BCR-C can sufficiently understand them. The same applies to any parts/version of the BCR-C that will be published with the aim of providing access to the BCR-C for data subjects.	
2 - SCOPE OF THE BCR					
2.1 Description of the material scope of the BCR-C	YES	YES	Article 47(2)(b) GDPR	In order to be transparent as to the scope of the BCRC, the BCR-C must specify their material scope, and therefore contain a description of the transfers.	

[6] See Section 2.1 below.

				The BCR-C must, in particular, specify per transfer or set of transfers[7] (for example, 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, customers, suppliers 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-C will apply to all data subjects whose personal data are transferred within the scope of the BCR-C from an entity under the scope of application of Chapter V GDPR. Therefore, the scope of the BCR-C may, in particular, not be limited to "EEA citizens or EEA residents".	
2.2 List of BCR members, and description of the geographical scope of the BCR-C	YES	YES	Article 47(2)(a) GDPR	The BCR-C shall specify the structure and contact details of the Group and of each of its BCR members (contact details of the BCR members – such as address and company registration number, where available – should be inserted in the list of BCR members that is part of the BCR-C, for example an annex thereof, that has to be published along with the BCR-C). The BCR-C should indicate that they at least apply to all personal data transferred to BCR members outside the EEA, and onward transfers to other BCR members outside the EEA.	
3 - EFFECTIVENESS					

[7] The information on the transfers must be exhaustive in that every 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-C updates applies, i.e., information on the amendments to the BCR-C must be provided in the annual BCR-C update notified to the BCR Lead (see Section 8.1 below).

3.1 Suitable training programme	YES	~~YES~~ ~~NO~~YES	Article 47(2)(n) GDPR	The BCR-C must state that appropriate and up-to-date training on the BCR-C 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-C are approved. In this regard it should be recalled that no transfer can be made under the BCR-C to a BCR member unless the member is effectively bound by the BCR-C and can deliver compliance (see Section 7.1) which includes that appropriate training on the BCR-C can effectively be provided to the employees of the respective member. Training intervals should be specified in the BCR-C. Training should cover, among others, procedures of managing requests for access to personal data by public authorities. The SAs evaluating the BCR-C may ask for examples and explanations of the training programme during the application procedure.	
3.2 Complaint handling process for the BCR-C	YES	~~YES~~ NO	Article 47(2)(i) and Article 12(3) GDPR	An internal complaint handling process must be set up in the BCR-C to ensure that any data subject should be able to exercise their rights and complain about any BCR member. ~~- The complaints must be dealt with, without undue delay~~The BCR-C (or, depending on the case, the parts of the BCR-C that will be published for the attention of data subjects, see Section 1.7 above) will include the point(s) of contact where data subjects can lodge any complaints related to the processing of their personal data covered by the BCR-C. A single point of contact or a number of points	

				of contact are possible. In this regard, a physical address should be provided. Additionally, further contact options may be provided, e.g. 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-C must contain the duty for the controller 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 ~~his/her~~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-C (or, depending on the case, the parts of the BCR-C that will be published for the attention of data subjects, see Section 1.7 above) should include information about the practical steps of the complaint process, in particular: - 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 Audit programme covering the BCR-C	YES	~~YES~~ NO	Article 47(2)(j) and (l), and Article 38(3) GDPR	The BCR-C 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-C. The audit frequency envisaged should be specified in the BCR-C. The frequency needs to be determined on the basis of the risk(s) posed by the processing activities covered by the BCR-C 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, the BCR-C should specify the conditions under which such auditors may be entrusted. The BCR-C should state which entity (department within the Group) decides on the audit plan/programme, and which entity will conduct the audit~~,~~. Data protection officers should not be the ones in charge of auditing compliance with the BCR-C, if such situation can result in a conflict of interests. Functions that may possibly be entrusted with deciding on the audit plan/programme and/or with conducting audits include, for instance, Audit Departments, but other appropriate solutions may be acceptable too provided that: - the persons in charge are guaranteed independence as to the performance of their duties related to these audits; and - the BCR-C include an explicit commitment in this regard. The BCR-C should state that the audit programme covers all aspects of the BCR-C (for instance, 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-C, review of the contractual terms used for the transfers out of the Group to controllers or processors of data, 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 BCRC each time a BCR member is audited, as long as all aspects of the BCR-C are monitored at appropriate regular intervals for that BCR member. Moreover, the BCR-C 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. The BCR-C must state that Competent SAs can have access to the results of the audit upon request. 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 BCRC 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.	
3.4 Creation of a network of data protection officers (DPOs) or appropriate	YES	NO	Article 47(2)(h) and Article 38(3) GDPR	The BCR-C must contain a commitment to designate a DPO, where required in line with Article 37 GDPR, or any other person or entity (such as a chief privacy officer) with responsibility to monitor compliance with the BCR-C,	

staff for monitoring compliance with the BCR-C				enjoying the highest management support for the fulfilling of this task. The DPO or the other privacy professionals 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 can inform the highest management level if any questions or problems arise during the performance of their duties. The BCR-C should 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-C. 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-C audits if such situations can result in a conflict of interests. However, the DPO can play a very important and useful role in assisting the BCR members, and the advice of the DPO should be sought for such tasks. The BCR-C should specify that the DPO or other privacy professionals may be directly contacted. The BCR-C should include a commitment to publish their contact details.	

4 - COOPERATION DUTY					
4.1 Duty to cooperate with Competent SAs	YES	~~YES~~ NO	Article 47(2)(l) and Article 31 GDPR	The BCR-C 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-C. The BCR-C shall include the obligation to provide the Competent SAs, upon request, with any information about the processing operations covered by the BCR-C. 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-C 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-C can neither 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-C need to include a commitment that any dispute related to the Competent SAs' exercise of supervision of compliance with the BCR-C will be resolved by the courts of 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.	
5 - DATA PROTECTION SAFEGUARDS					

5.1.1 Description of the data protection principles	YES	~~YES~~ NO	Article 47(2)(d) and Article 5 GDPR	The BCR-C should explicitly include and describe the following principles to be observed by the BCR members.
				The BCR-C need to establish those principles in a sufficiently elaborated manner that is in line with the content of the principles as provided for in the GDPR provisions.
				The BCR-C should not include general limitations to the application of these principles (e.g., pre-defined lists of overriding interests), which limitations can only be applied on a case-by case basis, and, where applicable, in accordance with the transparency requirements.
				i. **Transparency, fairness and lawfulness** (see Section 5.1.2 below) for processing of personal data, special categories of data, and data relating to criminal convictions and offences
				(see Article 5(1)(a), and Articles 6, 9, and 10 GDPR);
				ii. **Purpose limitation** (see Article 5(1)(b) GDPR);
				iii. **Data minimisation and accuracy** (see Article 5(1)(c) and (d) GDPR);
				iv. **Limited storage periods** (see Article 5(1)(e) GDPR);
				v. **Security** (integrity and confidentiality, see Section 5.1.3 below, and Article 5(1)(f) GDPR); and
				vi. **Onward transfers** (see Section 5.1.4 below and Chapter V GDPR).	

5.1.2 Lawfulness of processing	YES	~~YES~~ NO	Article 47(2)(d), Article 5(1)(a), and Articles 6 and 9 GDPR	The BCR-C should contain an exhaustive list of all legal basis for processing which the BCR members intend to rely on. Only legal basis as those stipulated in Article 6(1) and (3) GDPR, or in other legal basis laid down in Union or Member state law, as permitted by the GDPR, can be used.[8] In addition, special categories of personal data may only be processed if exemptions as the ones envisaged by Article 9(2) GDPR apply. The BCR-C should contain an exhaustive list of all such exemptions. Processing of personal data relating to criminal convictions and offences shall be prohibited, unless the same exemptions as the ones envisaged by Article 10 GDPR apply.	
~~.~~ 5.1.3 Security and personal data breach notifications	YES	~~YES~~ NO	Article 47(2)(d) and Articles 32 to 34 GDPR	The BCR-C should include a commitment to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk(s) for the rights and freedoms of natural persons (see Article 5(f) and Article 32 GDPR). It is not mandatory to copy-paste the wording of such GDPR provisions. However, the BCR-C need to create those obligations in a sufficiently elaborated manner that is in line with the content of these provisions. The BCR-C should include a duty to notify: - without undue delay, any personal data breaches to the Liable BCR member and the relevant Privacy officer or Function, as well as to the BCR member acting as a controller when a BCR member acting as a processor becomes aware of a data breach;	

[8] As regards possible conflicts with third country legal obligations, see Section 5.4.1 below.

				- without undue delay, and, where feasible, not later than 72 hours after having become aware of the personal data breach to the Competent SA, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons; - without undue delay to data subjects, where the personal data breach is likely to result in a high risk to their rights and freedoms in line with the requirements of Article 34 GDPR~~.~~. Furthermore, any personal data breach should be documented (comprising the facts relating to the personal data breach, its effects, and the remedial action taken~~)~~), and the documentation should be made available to the Competent SA upon request (see Articles 33 and 34 GDPR).	
5.1.4 Restrictions on onward transfers	YES	NO	Article 47(2)(d) GDPR and Article 44 GDPR	BCR-C should contain the commitment that personal data that have been transferred under the BCR may only be onward transferred outside the EEA to processors and controllers which are not bound by the BCR-C[9] if the conditions for transfers laid down in Articles 44 to 46 GDPR are applied in order to ensure that the level of protection of natural persons guaranteed by GDPR is not undermined. In the absence of an adequacy decision or appropriate safeguards, BCR-C may include a provision that onward transfers may exceptionally take place if a derogation applies in line with Article 49 GDPR.	
5.2 Rights of data subjects	YES	NO	Article 47(2)(e), Articles 12 to 19 and 21 to 22 GDPR	The BCR-C should provide data subjects with the rights of information, access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling, in the same way as these rights are	

[9] For onward transfers to other BCR members outside the EEA, see Section 2.2 above.

				provided for by Articles 12 to 19, and Articles 21 and 22 GDPR. It is not mandatory to copy-paste the wording of the above-mentioned GDPR provisions. However, the BCR-C need to create those rights in a sufficiently elaborated manner that is in line with the content of these provisions.	
5.3 Accountability and other tools	YES	~~YES~~ NO	Article 47(2)(d), and Articles 30, 35-36 GDPR	Every BCR member acting as controller shall be responsible for and able to demonstrate compliance with the BCR-C (see Article 5(2) and Article 24 GDPR). The BCR-C need to contain a commitment to enter into contracts with all internal and external processors and must specify the content of such contracts, as set out in Article 28(3) GDPR, including the duty to follow the controller's instructions and implement appropriate technical and organisational measures. The BCR-C 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 personal data transferred under these BCR-C. The BCR-C must specify the content of the record, in line with what is required by Article 30(1) (for controllers) and Article 30(2) (for processors). This record should be maintained in writing, including in electronic form, and should be made available to the Competent SA on request. The BCR-C should contain the commitment that data protection impact assessments should be carried out for processing operations on personal data transferred under these BCR-C that are likely to result in a high risk to the rights and freedoms of natural persons (see Article 35 GDPR). Where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the	

				BCR member acting as a controller should, prior to processing, consult the Competent SA (see Article 36 GDPR). The BCR-C should envisage that appropriate technical and organisational measures designed to implement data protection principles and to facilitate compliance, in practice, with the requirements set up by the BCR-C, should be implemented (data protection by design and by default – see Article 25 GDPR).	
~~6.3 The need to be transparent where national legislation prevents the group from complying with the BCRs~~ 5.4.1 Local laws and practices affecting compliance with the BCR-C[10]	YES	NO	Article 47(2)(m) GDPR	~~A~~ The BCR-C shall contain a clear commitment that BCR members will use the BCR-C as a tool for transfers only where ~~a BCR member has reasons to believe~~ they have assessed that the ~~legislation~~ law and practices in the third country of destination applicable to ~~him prevents the company~~ the processing of the personal data by the BCR member acting as data importer, including any requirements to disclose personal data or measures authorising access by public authorities, do not prevent it from fulfilling its obligations under these BCR-C. The BCR-C 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[11] to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the BCR-C. The BCR-C should also contain a commitment that, in assessing the laws and practices of the third country which	

[10] 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.

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

				may affect the respect of the commitments contained in the BCR-C, 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 relevant in light of the circumstances of the transfer[12], 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 country of the data importer, as well as the applicable limitations and safeguards[13].	

[12] 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, available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer en.

[13] As regards the impact of such laws and practices on compliance with the BCR, 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

				iii. ~~the BCRs~~ Any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the BCR-C, including measures applied during the transmission and to the processing of the personal data in the country of destination. The BCR-C should also contain a commitment that where any safeguards in addition to those envisaged under the BCR-C 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. The BCR-C should contain also an obligation for the BCR members to document appropriately such assessment, as well as the supplementary measures selected and implemented. They should make such documentation available to the competent SAs upon request. The BCR-C should oblige any BCR member acting as data importer to promptly notify the data exporter if, when using these BCR-Cas a tool for transfers, and for the duration of the BCR membership, it has reasons to believe that it is or has ~~substantial effect on the guarantees~~ become subject to laws or practices that would prevent it from fulfilling its obligations under the BCR-C, including following a change in the laws in the third country or a measure (such as a disclosure request). This information should also be provided ~~by the rules, he will promptly~~ to the Liable BCR member(s). Upon verification of such notification, the BCR member acting as data exporter, along with the Liable BCR	

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.

				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 order to enable them to fulfil their obligations under the BCR-C. 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-C. 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-C – even if accompanied by supplementary measures – cannot be complied with for a transfer or set of transfers, or if instructed by the Competent SAs, it commits to 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 again ensured or the transfer is ended. The BCR-C should contain a commitment that following such a suspension, the BCR member acting as data exporter has to end the transfer or set of transfers if the BCR-C 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 BCR member acting as data exporter, be returned to it or destroyed in their entirety. The BCR-C should contain a commitment that the liable BCR member(s) and the relevant Privacy officer or Function will inform ~~the EU headquarters or the EU BCR member with delegated data~~all other BCR members of the assessment carried out and of its results, so that the	

				identified supplementary measures will be applied 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-C needs to 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 ~~responsibilities and the other relevant Privacy Officer/Function (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).~~ and the decisions taken accordingly on such transfers.~~, the BCRs should contain a commitment that where any legal requirement a BCR member is subject to in a third country is likely to have a substantial adverse effect on the guarantees provided by the BCRs, the problem should be reported to the competent SA. This includes any legally binding request for disclosure of the personal data by a law enforcement authority or state security body. In such a case, the competent SA should be clearly informed about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).~~ ~~If in specific cases the suspension and/or notification are prohibited, the BCRs shall provide that the requested BCR member will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.~~ ~~If, in the above cases, despite having used its best efforts, the requested BCR member is not in a position to notify the~~	

				~~competent SAs, it must commit in the BCRs to annually providing general information on the requests it received to the competent SAs (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).~~ ~~In any case, the BCRs must state that transfers of personal data by a BCR member of the group to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.~~	
~~6.4 A statement about the relationship between national laws and BCRs~~ 5.4.2 Obligations of the data importer in case of government access requests	YES	NO	~~N/A~~ Article 47(2)(m) GDPR	Without prejudice to the obligation of the BCR member acting as data importer to inform the data exporter of its inability to comply with the commitments contained in the BCR-C (see Section 5.4.1 above), the BCR-C should also include the following commitments: i. The BCR member acting as data importer will promptly notify the data exporter 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 an another third country, for disclosure of personal data transferred pursuant to the BCR-C; 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-C 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 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, 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-C, 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. It will also make it available to the Competent SAs upon request. vii. ~~BCRs shall specify the relationship between the BCRs and the relevant applicable law.~~ 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-C 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 in a democratic society[14] (as to the consequences of such cases, see Section 5.4.1 above).~~BCRs shall state that, where the local legislation, for instance EU legislation, requires a higher level of protection for personal data it will take precedence over the BCRs. any event personal data shall be processed in accordance to the applicable law as provided by the Article 5 of the GDPR and the relevant local legislation.~~	
6 - TERMINATION					
6.1 Termination	YES	NO	Article 70(1)(i) GDPR	The BCR-C should specify that a BCR member acting as data importer, which ceases to be bound by the BCR-C may keep, return, or delete the personal data received under the BCR-C. If the data exporter and data importer agree that the data may be kept by the data importer, protection must be maintained in accordance with Chapter V GDPR.	

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

7 – NON-COMPLIANCE					
7.1. Non-Compliance	YES	NO	Article 70(1)(i) GDPR	The BCR-C 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-C and can deliver compliance. ii. The data importer should promptly inform the data exporter if it is unable to comply with the BCR-C, for whatever reason, including the situations further described under Section 5.4.1 above. iii. Where the data importer is in breach of the BCR-C or unable to comply with them, the data exporter should suspend the transfer. iv. The data importer should, at the choice of the data exporter, immediately return or delete the personal data that has been transferred under the BCR-C in its entirety, where: - the data exporter has suspended the transfer, and compliance with this BCRC 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-C; or -the data importer fails to comply with a binding decision of a competent court or Competent SA regarding its obligations under the BCR-C. 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-C. 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-C, 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-C, see Section 5.4.1 above.	
8 - MECHANISMS FOR REPORTING AND RECORDING CHANGES					
8.1 Process for updating the BCR-C	YES	NO	Article 47(2)(k) GDPR	The BCR-C have to be kept up-to-date in order to reflect the current situation (for instance to take into account modifications of the regulatory environment, these EDPB Recommendations, or changes to the scope of the BCR-C). The BCR-C should impose a duty to report changes, including to the list of BCR members, without undue delay, **to all BCR members.** The BCR-C 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-C, and provides the necessary information **to data subjects**, and, upon request, **to Competent SAs**. Where a modification to the BCR-C would possibly be detrimental to the level of the protection offered by the BCR-C or significantly affect them (e.g. changes to the binding character, change of the Liable BCR member(s)), it must be communicated in advance to the SAs, via the BCR Lead, with a brief explanation of the reasons for the	

				update. In this case, the SAs will also assess whether the changes made require a new approval. Once a year, the SAs should be notified via the BCR Lead of any changes to the BCR-C 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-C 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-C holder to keep it up-to-date and in compliance with Article 47 GDPR and these EDPB Recommendations.	
9 - DEFINITIONS					
9.1 List of definitions	YES	NO	Article 70(1)(i) GDPR	The applicant should include a list of definitions in the BCR-C. The list should include the most relevant terms. To the extent the BCR-C contain terms defined in the GDPR, the definitions provided should not vary from the GDPR. For better 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 the EEA data protection SA competent for the data exporter. 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 5.4.1 and 5.4.2 above. References to GDPR provisions should generally be avoided. However, if there is a need for reference to a particular provision of the GDPR, it should be quoted in full in the BCR-C.	

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Singapore • Stockholm • Sydney • Warsaw