18/EN
WP 256 rev.01

Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules

Adopted on 6 February 2018
As last Revised and Adopted on 28 November 2017

INTRODUCTION

In order to facilitate the use of Binding Corporate Rules for Controllers (BCR-C) by a corporate group or a group of enterprises engaged in a joint economic activity for international transfers from organisations established in the EU to organisations within the same group established outside the EU, the Article 29 Working Party (WP29) has amended the Working Document 153 (which was adopted in 2008) setting up a table with the elements and principles to be found in Binding Corporate Rules in order to reflect the requirements referring to BCRs now expressly set out by the Regulation (EU) 2016/679 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 (General Data Protection Regulation / GDPR)[1].

It should be recalled that BCR-Controllers are suitable for framing transfers of personal data from Controllers established in the EU to other Controllers or to Processors (established outside the EU) within the same group, whereas BCR-Processors (BCR-P) apply to data received from a Controller (established in the EU) which is not a member of the group and then processed by the concerned group members as Processors and/or Sub-processors. Hence the obligations set out in the BCR-C apply in relation to entities within the same group acting as controllers and to entities acting as 'internal' processors. As for this very last case, it is worth recalling that a contract or other legal act under Union or Member State law, binding on the processor with regard to the controller and which comprise all requirements as set out in Art. 28.3 GDPR, should be signed with all internal and external subcontractors/processors (e.g. Service Agreement or other instruments meeting the same requirements) [2]. Indeed, the obligations set forth in the BCR-C apply to entities of the group receiving personal data as ('internal') processors to the extent that this does not lead to a contradiction with the Service Agreement (i.e. the Processors members of the group processing on behalf of Controllers members of the group shall primarily abide by this contract).

Taking into account that Article 47.2 GDPR sets forth a minimum set of elements to be inserted within Binding Corporate Rules, this amended table is meant to:

- Adjust the wording of the previous referential so as to keep it in line with Article 47 GDPR,
- Clarify the necessary content of BCRs as stated in Article 47 (taking into account documents WP 74[3] & WP 108[4] adopted by the WP29 within the framework of the directive 95/46/EC),

[1] Text with EEA relevance.

[2] Art. 28.3 requires, among others, for each controller-to-processor relationship a specification, by way of contract or other legal act, of the subject-matter, the duration, the nature and purposes of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. A generic description included in the BCRs regarding the categories of data, data subjects etc. would not be sufficient in this regard.

[3] Working Document WP 74: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on June 3, 2003, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en htm

[4] Working Document WP 108: Establishing a model checklist application for approval of Binding Corporate Rules, adopted on April 14, 2005, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm

- Make the distinction between what must be included in BCRs and what must be presented to the competent Supervisory Authority in the BCRs application (document WP 133[5]),
- Give the principles the corresponding text references in Article 47 GDPR, and
- Provide explanations/comments on the principles one by one.

Article 47 GDPR is clearly modelled on the Working documents relating to BCRs adopted by the WP29. However, it specifies some new elements that need to be taken into account when updating already existing BCRs or adopting new sets of BCRs so as to ensure their compatibility with the new framework established by the GDPR.

1.1 New elements

In this perspective, the WP29 would like to draw attention in particular to the following elements:

- ***right to lodge a complaint***: Data subjects should be given the right to bring their claim, as they choose, either before the Supervisory Authority ('SA') in the Member State of his habitual residence, place of work or place of the alleged infringement (pursuant to Art. 77 GDPR) or before the competent court of the EU Member States (choice for the data subject to act before the courts where the data exporter has an establishment or where the data subject has his or her habitual residence (Article 79 GDPR);
- ***Transparency***: All data subjects benefitting from the third party beneficiary rights should in particular be provided with information as stipulated in Articles 13 and 14 GDPR and information on their rights in regard to processing and the means to exercise those rights, the clause relating to liability and the clauses relating to the data protection principles;
- ***Scope of application***: The BCRs shall specify the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity and of each of its members (GDPR Art. 47.2.a). The BCRs must also specify its material scope, for instance the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the types of data subjects affected and the identification of the third country or countries (GDPR Art. 47.2.b);
- ***Data Protection principles***: Along with the principles of transparency, fairness, purpose limitation, data quality, security, the BCRs should also explain the other principles referred to in Article 47.2.d – such as, in particular, the principles of lawfulness, data minimisation, limited storage periods, guarantees when processing special categories of personal data, the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
- ***Accountability***: Every entity acting as data controller shall be responsible for and able to demonstrate compliance with the BCRs (GDPR Art. 5.2);
- ***Third country legislation***: The BCRs should contain a commitment that where any legal requirement a member of the group of undertakings or group of enterprises

[5] Working Document WP 133: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data, adopted on January 10, 2007, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp133_en.doc

engaged in a joint economic activity is subject to in a third country is likely to have a substantial adverse effect on the guarantees provided by the BCRs, the problem will be reported to the competent supervisory authority (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). This includes any legally binding request for disclosure of personal data by a law enforcement authority or state security body.

1.2 Amendments of already adopted BCRs

While in accordance with article 46-5 of the GDPR, authorisations by a Member State or supervisory authority made on the basis of Article 26(2) of Directive 95/46/EC will remain valid until amended, replaced or repealed, if necessary, by that supervisory authority, groups with approved BCRs should, in preparing to the GDPR, bring their BCRs in line with GDPR requirements.

This document aims also to assist those groups with approved BCRs in implementing the relevant changes to bring them in line with the GDPR. To this end, these groups are invited to notify the relevant changes to their BCRs as part of their obligation (under 5.1 of WP153) to all group members and to the DPAs via the Lead DPA under their annual update as of 25 May 2018. Such updated BCRs can be used without having to apply for a new authorization or approval.

Taking into account the above, the DPAs reserve their right to exercise their powers under article 46-5 of the GDPR.

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
1 - BINDING NATURE					
INTERNALLY					
1.1 The duty to respect the BCRs	YES	YES	GDPR Art. 47.1.a and 47.2.c	The BCRs must be legally binding and shall contain a clear duty for each participating member of the Group of undertakings or group of enterprises engaged in a joint economic activity ('BCR member') including their employees to respect the BCRs.	
1.2 An explanation of how the rules are made binding on the BCR members of the group and also the employees	NO	YES	GDPR Art. 47.1.a and 47.2.c	The Group will have to explain in its application form how the rules are made binding : i) For each participating company/entity in the group by one or more of: - Intra-group agreement, - Unilateral undertakings (this is only possible if the BCR member taking responsibility and liability is located in a Member State that recognizes Unilateral undertakings as binding and if this BCR member is legally able to bind the other members subject to BCRs), - Other means (only if the group demonstrates how the binding character of the BCRs is achieved)	

[6] To be completed by applicant.

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
				ii) On employees by one or more of: - Individual and separate agreement(s)/undertaking with sanctions, - Clause in employment contract with a description of applicable sanctions, - Internal policies with sanctions, or - Collective agreements with sanctions - Other means (but the group must properly explain how the BCRs are made binding on the employees)	
EXTERNALLY					
1.3 The creation of third-party beneficiary rights for data subjects. Including the possibility to lodge a complaint before the competent SA and before the courts	YES	YES	GDPR Art. 47.1.b, and 47.2.c, 47.2.e	The BCRs must expressly confer rights on data subjects to enforce the rules as third-party beneficiaries. Data subjects must at least be able to enforce the following elements of the BCRs: - Data protection principles (Art. 47.2.d and Section 6.1 of this referential), - Transparency and easy access to BCRs (Art. 47.2.g and Section 6.1, Section 1.7 of this referential), - Rights of access, rectification, erasure, restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling (GDPR Art. 47.2.e and Art. 15, 16, 17,18, 21, 22),	

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
				- National legislation preventing respect of BCRs (Art. 47.2 m and Section 6.3 of this referential), - Right to complain through the internal complaint mechanism of the companies (Art. 47.1.i and Section 2.2 of this referential), - Cooperation duties with Supervisory Authorities (Art. 47.2 k and l, Section 3.1 of this referential), - Liability and jurisdiction provisions (Art. 47.2.e and f, Section 1.3, 1.4 of this referential). In particular, the BCRs must confer the right to lodge a complaint with the competent supervisory authority (choice before the SA in the Member State of his habitual residence, place of work or place of the alleged infringement, pursuant to art. 77 GDPR) and before the competent court of the EU Member States (choice for the data subject to act before the courts where the controller or processor has an establishment or where the data subject has his or her habitual residence pursuant to Article 79 GDPR). The BCRs should expressly confer to the 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 BCRs as enumerated above (see Articles 77 – 82 GDPR). Companies should ensure that all those rights are covered by the third party beneficiary clause of their BCRs by, for example, making a reference to the clauses/sections/parts of their BCRs where these rights are regulated or by listing them	

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
				all in the said third party beneficiary clause. These rights do not extend to those elements of the BCRs pertaining to internal mechanisms implemented within entities such as detail of training, audit programmes, compliance network, and mechanism for updating of the rules.	
1.4 The EU headquarters, EU member with delegated data protection responsibilities or the data exporter accepts liability for paying compensation and to remedy breaches of the BCRs.	YES	YES	GDPR Art. 47.2.f	The BCRs must contain a duty for the EU headquarters, or the EU BCR member with delegated responsibilities to accept responsibility for and to agree to take the necessary action to remedy the acts of other members outside of the EU bound by the BCRs and to pay compensation for any material or non-material damages resulting from the violation of the BCRs by BCR members. The BCRs must also state that, if a BCR member outside the EU violates the BCRs, the courts or other competent authorities in the EU will have jurisdiction and the data subject will have the rights and remedies against the BCR member that has accepted responsibility and liability as if the violation had been caused by them in the Member State in which they are based instead of the BCR member outside the EU. Another option, in particular if it is not possible for a group with particular corporate structures to impose on a specific entity to take all the responsibility for any breach of BCRs outside of the EU, it may provide that every BCR member exporting data out of the EU on the basis of the BCR will be liable for any breaches of the BCRs by the BCR member established outside the EU which received the data from this EU BCR	

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
				member.	
1.5 The company has sufficient assets.	NO	YES	[WP 74 point 5.5.2. §2 (page 18) + WP108 point 5.17. (page 6)]	The application form must contain a confirmation that any BCR member that has accepted liability for the acts of other members bound by the BCRs outside of the EU has sufficient assets to pay compensation for damages resulting from the breach of the BCRs.	
1.6 The burden of proof lies with the company not the individual.	YES	YES	GDPR Art. 47.2.f	BCRs must state that the BCR member that has accepted liability will also have the burden of proof to demonstrate that the BCR member outside the EU is not liable for any violation of the rules which has resulted in the data subject claiming damages. If the BCR member that has accepted liability can prove that the BCR member outside the EU is not responsible for the event giving rise to the damage, it may discharge itself from any responsibility.	

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
1.7 Transparency and easy access to BCRs for data subjects	YES	NO	GDPR Art. 47.2.g	BCRs must contain the commitment that all data subjects benefitting from the third party beneficiary rights 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, the clause relating to the liability and the clauses relating to the data protection principles. The information should be provided in full and a summary will not be sufficient .. The BCRs must contain the right for every data subject to have an easy access to them. For instance, the BCRs may state that at least the parts of the BCRs on which information to the data subjects is mandatory (as described in the previous paragraph) will be published on the internet or on the intranet (when data subjects are only the company staff having access to the intranet).	
2 - EFFECTIVENESS					
2.1 The existence of a suitable training programme	YES	YES	GDPR 47.2.n	The BCRs must state that appropriate training on the BCRs will be 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 Supervisory Authorities evaluating the BCRs may ask for examples and explanations of the training programme during the application procedure. The training programme should be specified in the application.	

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
2.2 The existence of a complaint handling process for the BCRs	YES	YES	GDPR 47.2.i and 12.3	An internal complaints handling process must be set up in the BCRs to ensure that any data subject should be able to exercise his/her rights and complain about any BCR member. - The complaints must be dealt with, 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 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 data subject should be informed accordingly.The application form must explain how data subjects will be informed about the practical steps of the complaint system, in particular: - Where to complain, - In what form, - Delays for the reply on the complaint, - Consequences in case of rejection of the complaint, - Consequences in case the complaint is considered as justified, - Consequences if the data subject is not satisfied by the replies (right to lodge a claim before the Court and a complaint before the Supervisory Authority) .	

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
2.3 The existence of an audit programme covering the BCRs	YES	YES	GDPR Art. 47.2.j and 1 and Art. 38.3,	The BCRs must create a duty for the group to have data protection audits on regular basis (by either internal or external accredited auditors) or on specific request from the privacy officer/function (or any other competent function in the organization) to ensure verification of compliance with the BCRs. The BCRs must state that the audit programme covers all aspects of the BCRs including methods of ensuring that corrective actions will take place. Moreover, the BCRs must state that the result will be communicated to the privacy officer/function and to the relevant board of the controlling undertaking of a group or of the group of enterprises engaged in a joint economic activity. Where appropriate, the result may be communicated to the ultimate parent's board. The BCRs must state that Supervisory Authorities can have access to the results of the audit upon request and give the SAs the authority/power to carry out a data protection audit of any BCR member if required. The application form will contain a description of the audit system. For instance : - Which entity (department within the group) decides on the audit plan/programme, - Which entity will conduct the audit, - Time of the audit (regularly or on specific request from the appropriate Privacy function.) - Coverage of the audit (for instance, applications, IT systems, databases that	

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
				process Personal Data, or onward transfers, decisions taken as regards mandatory requirement under national laws that conflicts with the BCRs, review of the contractual terms used for the transfers out of the Group (to controllers or processors of data), corrective actions, …) - Which entity will receive the results of the audits	
2.4 The creation of a network of data protection officers (DPO) or appropriate staff for monitoring compliance with the rules.	YES	NO	GDPR Art. 47.2.h and Art. 38.3	A commitment to designate a DPO where required in line with article 37 of the GDPR or any other person or entity (such as a chief privacy officer) with responsibility to monitor compliance with the BCRs 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. The DPO shall directly report to the highest management level (GDPR Art. 38-3). The BCRs 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 rules. For example, that the DPO or chief privacy officer informs and advises the highest management, deals with Supervisory Authorities' 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.	
3 - COOPERATION DUTY					

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
3.1 A duty to cooperate with SAs	YES	YES	GDPR Art. 47. 2.l	The BCRs should contain a clear duty for all BCR members to co-operate with, to accept to be audited by the Supervisory Authorities and to comply with the advice of these Supervisory Authorities on any issue related to those rules.	
4 - DESCRIPTION OF PROCESSING AND DATA FLOWS					
4.1 A description of the material scope of the BCRs (nature of data transferred, type of data subjects, countries)	YES	YES	GDPR Art. 47.2.b	The BCRs must specify their material scope and therefore contain a general description of the transfers so as to allow the Supervisory Authorities to assess that the processing carried out in third countries is compliant. The BCRs must in particular, specify the data transfers or set of transfers, including the nature and categories of personal data, the type of processing and its purposes, the types of data subjects affected (data related to employees, customers, suppliers and other third parties as part of its respective regular business activities) and the identification of the third country or countries.	
4.2 A statement of the geographical scope of the BCRs	YES	YES	GDPR art 47.2.a	The BCRs shall specify the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity and of each of its Members. The BCRs should indicate if they apply to: i) All personal data transferred from the European Union within the group OR, ii) All processing of personal data within the group	
5 - MECHANISMS FOR REPORTING AND RECORDING CHANGES					

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
5.1 A process for updating the BCRs	YES	YES	GDPR Art. 47.2.k	The BCRs can be modified (*for instance to take into account modifications of the regulatory environment or the company structure*) but they should impose a duty to report changes without undue delay to all BCR members and to the relevant Supervisory Authorities, via the competent Supervisory Authority. Updates to the BCRs or to the list of the Members of the BCRs are possible without having to re-apply for an approval providing that: i) An identified person or team/department keeps a fully updated list of the BCR members and keeps track of and record any updates to the rules and provide the necessary information to the data subjects or Supervisory Authorities upon request. ii) No transfer is made to a new BCR member until the new BCR member is effectively bound by the BCRs and can deliver compliance. iii) Any changes to the BCRs or to the list of BCR members should be reported once a year to the relevant SAs, via the competent SA with a brief explanation of the reasons justifying the update. iv) Where a modification would possibly affect the level of the protection offered by the BCRs or significantly affect the BCRs (i.e. changes to the binding character), it must be promptly communicated to the relevant Supervisory Authorities, via the competent SA.	
6 - DATA PROTECTION					

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
SAFEGUARDS					
6.1.1 A description of the data protection principles including the rules on transfers or onward transfers out of the EU.	YES	YES	GDPR art. 47.2.d	The BCRs should explicitly include the following principles to be observed by the company: i. Transparency, fairness and lawfulness (GDPR Art. 5.1.a, 6, 9, 10, 13 and 14) ii. Purpose limitation (GDPR Art.5.1.b) iii. Data minimisation and accuracy (GDPR Art. 5.1.c and d) iv. Limited storage periods (GDPR Art. 5.1.e) v. Processing of special categories of personal data vi. Security (GDPR Art. 5.f and 32) including the obligation to enter into contracts with all internal and external subcontractors/processors which comprise all requirements as set out in Art. 28.3 GDPR and as well the duty to notify without undue delay any personal data breaches to the EU headquarters or the EU BCR member with delegated data protection responsibilities and the other relevant Privacy Officer/Function and data subjects where the personal data breach is likely to result in a high risk to their rights and freedoms . Furthermore, any personal data breaches 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 supervisory authority on request (GDPR Art. 33 and 34). vii. Restriction on transfers and onward transfers to processors and controllers which are not part of the group (BCR members that are controllers can transfer data to processors/controllers out of the group that are	

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
				located outside of the EU provided that adequate protection is provided according to Articles 45, 46, 47 48 GDPR, or that a derogation according to 49 GDPR applies) The wording and definitions of the BCRs key principles should be consistent with the wording and definitions of the GDPR.	
6.1.2 Accountability and other tools	YES	YES	GDPR Art. 47.2.d and Art. 30	Every entity acting as data controller shall be responsible for and able to demonstrate compliance with the BCRs (GDPR Art. 5.2 and 24). In order to demonstrate compliance, BCR members need to maintain a record of all categories of processing activities carried out in line with the requirements as set out in Art. 30.1 GDPR. This record should be maintained in writing, including in electronic form, and should be made available to the supervisory authority on request. In order to enhance compliance and when required, data protection impact assessments should be carried out for processing operations that are likely to result in a high risk to the rights and freedoms of natural persons (GDPR Art. 35). Where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the competent supervisory authority, prior to processing, should be consulted (GDPR Art. 36). Appropriate technical and organisational measures should be implemented which are designed to	

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
				implement data protection principles and to facilitate compliance with the requirements set up by the BCRs in practice (data protection by design and by default (GDPR Art. 25)	
6.2 The list of entities bound by BCRs	YES	YES	GDPR 47.2.a	BCR shall contain a list of the entities bound by the BCRs including contact details.	
6.3 The need to be transparent where national legislation prevents the group from complying with the BCRs	YES	NO	GDPR Art. 47.2.m	A clear commitment that where a BCR member has reasons to believe that the legislation applicable to him prevents the company from fulfilling its obligations under the BCRs or has substantial effect on the guarantees provided by the rules, he will promptly inform the EU headquarters or the EU BCR member with delegated data 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). In addition, 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	

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
				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.	

Criteria for approval of BCRs	In the BCRs	In the application form	Texts of reference	Comments	References to application/BCRs[6]
6.4 A statement about the relationship between national laws and BCRs	YES	NO	N/A	BCRs shall specify the relationship between the BCRs and the relevant applicable law. The 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. In 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.	