18/EN
WP 257 rev.01

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

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

INTRODUCTION

In order to facilitate the use of Binding Corporate Rules for Processors (BCR-P) 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 195 (which was adopted in 2012) 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 in 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).

It should be recalled that 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 group members as processors and/or sub processors; whereas BCRs for Controllers (BCR-C) 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. Hence the obligations set out in the BCR-P apply in relation to third party personal data that are processed by a member of the group as a processor according to the instructions from a non-group controller.

According to Article 28.3 of the GDPR, a contract or another legal act under Union or Member State law that is binding on the processor with regard to the controller must be implemented between the controller and the processor. Such a contract or other legal act will be referred here as the "service agreement"..

Taking into account that Article 47.2 of the GDPR lists a minimum set of elements to be contained within a BCR, this amended table is meant to:

- Adjust the wording of the previous referential so as to bring it in line with Article 47 GDPR,
- Clarify the necessary content of a BCR as stated in Article 47 and in document WP 204[1] adopted by the WP29 within the framework of the Directive 95/46/EC,
- 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 195a[2]), and
- Provide explanations/comments on each of the requirements.

Article 47 of the 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 approved BCRs or adopting new sets of BCRs so as to ensure their compatibility with the new framework established by the GDPR.

1. New elements

[1] Working Document WP204: Explanatory Document on the Processor Binding Corporate Rules, as last revised and adopted on 22 May 2015

[2] Working Document WP 195a: Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities, adopted on 17 September 2012

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

- ***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 (Art. 47.2.a GDPR). The BCRs must also provide 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 (Art. 47.2.b GDPR);

- ***Third party beneficiary rights***: Data subjects should be able to enforce the BCRs as third party beneficiaries directly against the processor where the requirements at stake are specifically directed to processors in accordance with the GDPR (Art. 28, 29, 79 GDPR);

- ***Right to lodge a complaint***: Data subjects should be given the right to bring their claim, at their choice, either before the Supervisory Authority ('SA') in the Member State of his habitual residence, place of work or place of the alleged infringement (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);

- ***Data Protection principles***: Along with the obligations arising from principles of transparency, fairness, lawfulness, purpose limitation, data quality, security, the BCRs should also explain how other requirements, such as, in particular, in relation to data subjects rights, sub-processing and onward transfers to entities not bound by the BCRs will be observed by the processor;

- ***Accountability***: Processors will have an obligation to make available to the controller all information necessary to demonstrate compliance with their obligations including through audits and inspections conducted by the Controller or an auditor mandated by the Controller (Art. 28-3-h GDPR);

- ***Service Agreement***: The Service Agreement between the Controller and the Processor must contain all required elements as provided by Article 28 of the GDPR.

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 WP195) 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 from the DPAs.

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	Comments	References to Application/BCRs
1 - BINDING NATURE				
INTERNALLY				
1.1 The duty to respect the BCRs	YES	YES	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. The BCRs shall also expressly state that each 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 Service Agreement (Art. 28, 29 and 32 of the GDPR).	
1.2 An explanation of how the rules are made binding on the members of the group and also the employees	NO	YES	The Group will have to explain in its application form how the rules are made binding : i) For each BCR member 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 BCR members), or - Other means (only if the group demonstrates how bindingness is achieved). ii) On employees by one or more of: - Individual and separate agreement/undertaking with sanctions, or Clause in employment contract with sanctions, or - Internal policies with sanctions, or - Collective agreements with sanctions, or - Other means (but the group must properly explain how the BCRs are made binding on the employees).	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
EXTERNALLY				
1.3 The creation of third-party beneficiary rights for data subjects, including the possibility to lodge a complaint before the competent Supervisory Authorities and before the Courts	YES	YES	i) Rights which are directly enforceable against the processor The BCRs must grant rights to data subjects to enforce the BCRs as third party beneficiaries directly against the processor where the requirements at stake are specifically directed to processors in accordance with the GDPR. In this regard, data subjects shall at least be able to enforce the following elements of the BCRs directly against the processor: - Duty to respect the instructions from the controller regarding the data processing including for data transfers to third countries (Art. 28.3.a, 28.3.g., 29 GDPR and section 1.1, 6.1.ii and 6.1.iv of this referential), - Duty to implement appropriate technical and organizational security measures (Art. 28.3.c and 32 GDPR and section 6.1.iv of this referential) and duty to notify any personal data breach to the controller (Art. 33.2 GDPR and section 6.1.iv of this referential), - Duty to respect the conditions when engaging a sub-processor either within or outside the Group (Art. 28.2, 28.3.d . 28.4, 45, 46, 47 GDPR, section 6.1.vi and 6.1.vii of this referential), Duty to cooperate with and assist the controller in complying and demonstrating compliance with the law such as for answering requests from data subjects in relation to their rights (Art. 28.3.e, 28.3.f, 28.3.h and sections 3.2, 6.1.i, 6.1.iii, 6.1.iv, 6.1. v and 6.1. 2 of this referential) - Easy access to BCRs (Art.47.2.g GDPR and section 1.8 of this referential) - Right to complain through internal complaint mechanisms (Art.47.2.i and section 2.2 of this referential).	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			- Duty to cooperate with the supervisory authority (Art. 31, 47.2.l of GDPR and section 3.1 of this referential) - Liability, compensation and jurisdiction provisions (Art.47.2.e, 79, 82 GDPR and sections 1.3, 1.5 and 1.7 of this referential). - National legislation preventing respect of BCRs (Art.47.2.m and section 6.3 of this referential) ii) Rights which are enforceable against the processor in case the data subject is not able to bring a claim against the controller : The BCRs must expressly confer rights to data subjects to enforce the BCRs as third-party beneficiaries in case the data subject is not able to bring a claim against the data controller; because the data controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the data controller by contract of by operation of law, in which case the data subject can enforce its rights against such entity. In such a case, data subjects shall at least be able to enforce against the processor the following sections set out in this referential: 1.1, 1.3, 1.5, 1.7, 1.8, 2.2, 3.1, 3.2, 6.1, 6.2, 6.3 The data subjects' rights as mentioned under i) and ii) shall cover the judicial remedies for any breach of the third party beneficiary rights guaranteed and the right to obtain redress and where appropriate receive compensation for any damage (material harm but also any distress). In particular, data subjects shall be entitled to lodge a complaint before the competent supervisory authority (choice between the supervisory authority of the EU Member State of his/her habitual residence, place of work or place of alleged infringement) and before the competent court of the EU Member State (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 of the	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			GDPR). 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 (Art. 82.4 GDPR)	
1.4. Responsibility towards the Controller	YES	YES	The BCRs shall be made binding towards the Controller through a specific reference to it in the Service Agreement which shall comply with art 28 of the GDPR. Moreover, the BCR must state that the Controller shall have the right to enforce the BCR against any BCR member for breaches they caused, and, moreover, against the BCR member referred under point 1.5 in case of a breach of the BCRs or of the Service Agreement by BCR members established outside of EU or of a breach of the written agreement referred under 6.1.vii, by any external sub-processor established outside of the EU.	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
1.5 The company accepts liability for paying compensation and to remedy breaches of the BCRs.	YES	YES	The BCRs must contain a duty for the EU headquarters of the Processor or the EU BCR member of the Processor with delegated data protection responsibilities or the EU exporter Processor (e.g. the EU party contracting with the controller) to accept responsibility for and to agree to take the necessary action to remedy the acts of other BCR members established outside of EU or breaches caused by external sub-processor established outside of EU and to pay compensation for any damages resulting from a violation of the BCRs. This BCR member will accept liability as if the violation had taken place by him in the Member State in which he is based instead of the BCR member outside the EU or the external sub-processor established outside of EU. This 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. If it is not possible for some groups with particular corporate structures to impose all the responsibility for any type of breach of the BCRs outside of the EU on a specific entity, another option may consist of stating that each and every BCR member exporting data out of the EU will be liable for any breaches of the BCR by the sub-processors (internal or external of the group) established outside the EU which received the data from this EU BCR member.	
1.6 The company has sufficient assets.	NO	YES	The application form must contain a confirmation that any BCR member that has accepted liability for the acts of other BCR members outside of EU and/or for any external sub-processor established outside of EU has sufficient assets to pay compensation for damages resulting from the breach of the BCRs.	
1.7 The burden of proof lies with the company not the individual.	YES	YES	The BCRs must state that the BCR member that has accepted liability will have the burden of proof to demonstrate that the BCR member outside the EU or the external sub-processor is not liable for any violation of the rules which has resulted in the data subject claiming damages The BCRs must also state that where the Controller can demonstrate that	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			it suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of BCRs, it will be for the BCR member of the group that accepted liability to prove that the BCR member outside of the EU or the external sub-processor was not responsible for the breach of the BCRs giving rise to those damages or that no such breach took place If the entity that has accepted liability can prove that the BCR member outside the EU is not responsible for the act, it may discharge itself from any responsibility/liability.	
1.8 There is easy access to BCRs for data subjects and in particular easy access to the information about third party beneficiary rights for the data subject that benefit from them.	YES	NO	Access for the Controller: The Service Agreement will ensure that the BCRs are part of the contract. BCRs will be annexed to the Service Agreement or a reference to it will be made with a possibility of electronic access. Access for Data Subjects: BCRs must contain the commitment that all data subjects benefiting from the third party beneficiary rights should, in particular, be provided with the 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 BCRs must stipulate the right for every data subject to have easy access to them. Relevant parts of the BCRs shall be published on the website of the Processor Group or other appropriate means in a way easily accessible to data subjects or at least a document including **all** (and not a summary of) the information relating to points 1.1, 1.3, 1.4, 1.6, 1.7, 2.2, 3.1, 3.2, 4.1, 4.2, 6.1, 6.2, 6.3 of this referential.	
2 – EFFECTIVENESS				
2.1 The existence of a suitable training programme	YES	YES	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 personal data or in the development of tools used to process personal data. The Supervisory Authorities evaluating the BCRs may ask for some examples and explanation of the training programme during the application procedure and the training programme shall be specified in the application.	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
2.2 The existence of a complaint handling process for the BCRs	YES	YES	The BCRs shall contain a commitment from the Processor Group to create a specific contact point for data subjects. All BCR members shall have the duty to communicate a claim or request without undue delay to the Controller without obligation to handle it, (except if it has been agreed otherwise with the Controller). The BCRs shall contain a commitment for the Processor to handle complaints from data subjects where the Controller has disappeared factually or has ceased to exist in law or became insolvent. In all cases where the processor handles complaints, these shall be dealt without undue delay and in any event within one month by a clearly identified department or person who has an appropriate level of independence in the exercise of his/her functions. Taking into account the complexity and number of the requests, that period may be extended by two further months at the utmost, 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/Supervisory Authority)	
2.3 The existence of an audit programme covering the BCRs	YES	YES	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 the verification of compliance with the BCRs. The BCRs must state that the audit programme covers all aspects of the	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			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 but also will be made accessible to the Controller. Where appropriate, the result may be communicated to the ultimate parent's board. The BCRs must state that the Supervisory Authorities competent for the Controller can have access to the results of the audit upon request and give the Supervisory Authorities the authority/power to carry out a data protection audit of any BCR member if required. Any processor or sub-processor processing the personal data on behalf of a particular controller will accept, at the request of that controller, to submit their data processing facilities for audit of the processing activities relating to that controller which shall be carried out by the controller or an inspection body composed of independent members and in possession of the required professional qualifications, bound by a duty of confidentiality, selected by the data controller, where applicable, in agreement with the Supervisory Authority. 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 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.	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
2.4 The creation of a network of data protection officers (DPO) or appropriate staff for monitoring compliance with the rules	YES	NO	A commitment to appoint 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. This person/entity shall enjoy the highest management support in exercising this function. The DPO or other person/entity as mentioned, respectively, can be assisted, in exercising this function, 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). A brief description of the internal structure, role, position and tasks of the DPO or similar function, as mentioned, and the team/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 BCRs compliance at a global level, and that local DPOs or local contacts are in charge of reporting major privacy issues to the DPO or chief privacy officer, monitoring training and compliance at a local level.	
3 – COOPERATION DUTY				
3.1 A duty to cooperate with Supervisory Authorities	YES	YES	The BCRs shall contain a clear duty for all BCR members to cooperate with and to accept to be audited by the Supervisory Authorities competent for the relevant controller and to comply with the advice of these Supervisory Authorities on any issue related to those rules.	
3.2 A duty to cooperate with the Controller	YES	YES	The BCRs shall contain a clear duty for any processor or sub-processor to co-operate and assist the Controller to comply with data protection law (such as its duty to respect the data subject rights or to handle their complaints, or to be in a position to reply to investigation or inquiry from Supervisory Authorities). This shall be done in a reasonable time and to the extent reasonably possible.	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
4 – DESCRIPTION OF PROCESSING AND DATA FLOWS				
4.1 A description of the transfers and material scope covered by the BCRs	YES	YES	The BCRs shall contain a list of BCR members, i.e. entities that are bound by the BCRs (see also point 6.2) The Processor submitting a BCR shall give a general description to the Supervisory Authority of the material scope of the BCRs (expected nature of the data transferred, categories of personal data, types of data subjects concerned by the transfers, anticipated types of processing and its purposes.	
4.2 A statement of the geographical scope of the BCRs (nature of data, type of data subjects, countries)	YES	YES	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 the BCR members. The BCRs shall indicate that it is up to the Controller to apply the BCRs to: i) All personal data processed for processor activities and that are submitted to EU law (for instance, data has been transferred from the European Union), OR; ii) All processing of data processed for processor activities within the group whatever the origin of the data.	
5 - MECHANISMS FOR REPORTING AND RECORDING CHANGES				
5.1 A process for updating the BCRs	YES	YES	The BCRs can be modified (for instance to take into account modifications of the regulatory environment or the company structure) but they shall impose a duty to report changes to all BCR members, and to the relevant Supervisory Authorities, via the competent Supervisory Authorities 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 (for instance, on any intended changes concerning the addition or replacement of subcontractors, before the data	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			are communicated to the new sub-processor). Updates to the BCRs or to the list of the BCR members 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 of the sub-processors involved in the data processing activities for the controller which shall be made accessible to the data controller, data subject and Supervisory Authorities. ii) This person will keep track of and record any updates to the rules and provide the necessary information systematically to the data controller and upon request to Supervisory Authorities upon request. iii) No transfer is made to a new BCR member until the new BCR member is effectively bound by the BCR and can deliver compliance. iv) Any changes to the BCRs or to the list of BCR members shall be reported once a year to the relevant Supervisory Authorities, via the competent Supervisory Authority with a brief explanation of the reasons justifying the update. v) Where a modification would affect the level of the protection offered by the BCRs or significantly affect the BCRs (i.e. changes in the bindingness), it must be promptly communicated to the relevant Supervisory Authorities via the competent Supervisory Authority.	
6 - DATA PROTECTION SAFEGUARDS				
6.1 A description of the privacy principles including the rules on transfers or onward transfers outside of the EU	YES	YES	The BCRs shall include the following principles to be observed by any BCR member: i) Transparency, fairness, and lawfulness: Processors and sub-processors will have a general duty to help and assist the controller to comply with the law (for instance, to be transparent about sub-processor	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			activities in order to allow the controller to correctly inform the data subject); ii) Purpose limitation: duty to process the personal data only on behalf of the controller and in compliance with its documented instructions including with regard to transfers of personal data to a third country, unless required to do so by Union or Member State law to which the processor is subject. In such a case, the processor shall inform the controller of that legal requirement before processing takes place, unless that law prohibits such information on important grounds of public interest (Art. 28-3-a of the GDPR). In other cases, if the processor cannot provide such compliance for whatever reasons, it agrees to inform promptly the data controller of its inability to comply, in which case the controller is entitled to suspend the transfer of data and/or terminate the contract. On the termination of the provision of services related to the data processing, the processors and sub-processors shall, at the choice of the controller, delete or return all the personal data transferred to the controller and delete the copies thereof and certify to the controller that it has done so, unless legislation imposed upon them requires storage of the personal data transferred. In that case, the processors and the sub-processors will inform the controller and warrant that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore. iii) Data quality: Processors and sub-processors will have a general duty to help and assist the controller to comply with the law, in particular: - Processors and sub-processors will execute any necessary measures when asked by the Controller, in order to have the data updated, corrected or deleted. Processors and sub-processors will inform each BCR member to whom the data have been disclosed of any rectification, or deletion of data.	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			- Processors and sub-processors will execute any necessary measures, when asked by the Controller, in order to have the data deleted or anonymised from the moment the identification form is not necessary anymore. Processor and sub-processors will communicate to each entity to whom the data have been disclosed of any deletion or anonymisation of data. iv) Security: Processors and sub-processors will have a duty to implement all appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the processing as provided by Article 32 of the GDPR. Processors and sub-processors will also have a duty to assist the Controller in ensuring compliance with the obligations as set out in Articles 32 to 36 of the GDPR taking into account the nature of processing and information available to the processor (Art.28-3-f of the GDPR). Processors and sub-processors must implement technical and organisational measures which at least meet the requirements of the data controller's applicable law and any existing particular measures specified in the Service Agreement. Processors shall inform the Controller without undue delay after becoming aware of any personal data breach. In addition, sub-processors shall have the duty to inform the Processor and the Controller without undue delay after becoming aware of any personal data breach. v) Data subject rights: Processors and sub-processors will execute any appropriate technical and organizational measures, insofar as this is possible, when asked by the controller, for the fulfilment of the controller's obligations to respond to requests for exercising the data subjects rights as set out in Chapter III of the GDPR (Art. 28-3-e of the GDPR) including by communicating any useful information in order to help the controller to comply with the duty to respect the rights of the data subjects. Processor and sub-processors will transmit to the controller any data subject request without answering it unless he is authorised to do so.	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			vi) Sub-processing within the Group: data may be sub-processed by other BCR members bound by the BCRs only with the prior informed specific or general written authorization of the controller[3]. The Service 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 sub-processor. If a general authorization is given, the controller should be informed by the processor of any intended changes concerning the addition or replacement of a sub-processor 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 sub-processor. vii) Onward transfers to external sub-processors: Data may sub processed by non-members of the BCRs only with the prior informed specific or general written authorization of the controller[4]. If a general authorization is given, the controller should be informed by the processor of any intended changes concerning the addition or replacement of sub-processors 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 sub-processor. Where the BCR member bound by the BCRs subcontracts its obligations under the Service Agreement, with the authorization of the controller, it shall do so only by way of a contract or other legal act under Union or Member State law with the sub-processor which provides that adequate protection is provided as set out in Articles 28, 29, 32, 45, 46, 47 of the GDPR and which ensures that the same data protection obligations as set	

[3] Information on the main elements (parties, countries, security, guarantees in case of international transfers, with a possibility to get a copy of the contracts used). The detailed information, for instance relating to the name of the sub-processors could be provided e.g. in a public digital register.
[4] Information on the main elements (parties, countries, security, guarantees in case of international transfers, with a possibility to get a copy of the contracts used). The detailed information, for instance relating to the name of the sub-processors could be provided e.g. in a public digital register.

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			out in the Service Agreement between the controller and the processor and sections 1.3, 1.4, 3 and 6 of this referential are imposed on the sub-processor, in particular providing sufficient guarantees to implement appropriate technical and organization measures in such a manner that the processing will meet the requirements of the GDPR (Art. 28-4 of the GDPR).	
6.1.2 Accountability *and other tools*	YES	YES	Processors will have a duty to make available to the controller all information necessary to demonstrate compliance with their obligations as provided by Article 28-3-h of the GDPR and allow for and contribute to audits, including inspections conducted by the controller or another auditor mandated by the controller. In addition, the processor shall immediately inform the controller if in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. In order to demonstrate compliance with the BCRs, BCR members need to maintain a record of all categories of processing activities carried out on behalf of each controller in line with the requirements as set out in Art. 30.2 GDPR. This record should be maintained in writing, including in electronic form and should be made available to the supervisory authority on request (Art.30.3 and 30.4 GDPR) The BCR members shall also assist the controller in implementing appropriate technical and organisational measures to comply with data protection principles and facilitate compliance with the requirements set up by the BCRs in practice such as data protection by design and by default (Art. 25 and 47.2.d GDPR)	
6.2 The list of entities bound by BCRs	YES	YES	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	A clear commitment that where a BCR member has reasons to believe that the existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the controller or its obligations under the BCRs or Service Agreement, it will promptly notify this to the controller which is entitled to suspend the transfer of data and/or terminate the contract, to the EU headquarter processor or EU member	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			with delegated data protection responsibilities or the other relevant Privacy Officer/function, but also to the Supervisory Authority competent for the controller and the Supervisory authority competent for the processor. Any legally binding request for disclosure of the personal data by a law enforcement authority or state security body shall be communicated to the controller unless otherwise prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In any case, the request for disclosure should be put on hold and the Supervisory Authority competent for the controller and the competent Supervisory Authority for the processor should be clearly informed about the request, including information about the data requested, the requesting body and the legal basis for disclosure (unless otherwise prohibited). 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 provide 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	YES	NO	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	

Criteria for approval of BCRs	In the BCRs	In the application form	Comments	References to Application/BCRs
			legislation, requires a higher level of protection for personal data it will take precedence over the BCRs. In any event data shall be processed in accordance with the applicable law.	

II. COMMITMENTS TO BE TAKEN IN THE SERVICE LEVEL AGREEMENT

The BCRs for Processors shall unambiguously be linked to the Service Level Agreement signed with each Client. To that extent, it is important to make sure in the Service Level Agreement, which must contain all required elements provided by Article 28 of the GDPR, that:

- BCRs will be made enforceable for the Controller (Client) through a specific reference to it in the SLA (as an annex).
- The Controller shall commit that if the transfer involves special categories of data the Data Subject has been informed or will be informed before the transfer that his data could be transmitted to a third country not providing adequate protection;
- The Controller shall also commit to inform the data subject about the existence of processors based outside of EU and of the BCRs. The Controller shall make available to the Data Subjects upon request a copy of the BCRs and of the service agreement (without any sensitive and confidential commercial information);
- Clear confidentiality and security measures are described or referred with an electronic link;
- A clear description of the instructions and the data processing;
- The service agreement will specify if data may be sub-processed inside of the Group or outside of the group and will specify if the prior authorization to it expressed by the controller is general or needs to be given specifically for each new sub-processing activities.