ARTICLE 29 Data Protection Working Party

17/EN
WP264

Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data

Adopted on 11 April 2018

Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data[1]

Introduction and Instructions

The General Data Protection Regulation (EU) 2016/679 ('GDPR') allows personal data to be transferred outside the EEA only when the third country provides an "adequate level of protection" for the data (Art. 45) or when the controller adduces adequate safeguards with respect to the protection of privacy (Art. 46). Binding Corporate Rules (BCRs) are one of the ways in which such adequate safeguards (Art. 47) may be demonstrated by a group of undertakings, or group of enterprises engaged in a joint economic activity.

According to Article 64 GDPR, the use of BCRs as appropriate safeguards for international data transfers from the EEA requires the approval of the competent supervisory authority in accordance with the consistency mechanism set out in Article 63 without requiring any specific authorisation from a supervisory authority (Article 46.2.b GDPR). The following form is for use by companies seeking approval of BCRs. The form is based on papers previously issued by the Article 29 Working Party of European data protection authorities (the "Working Party"), and in particular WP133, and it is intended to help applicants demonstrate how to meet the requirements set out in Article 47 GDPR and WP 256.

General Instructions

- Only a single copy of the form need be filled out and submitted to the Supervisory Authority ('SA') you consider to be the lead authority for the BCRs ('BCR lead') in accordance with Article 47.1 and 64 GDPR and WP 263; this form may be used in all EEA Member States.
- Please fill out all entries and submit the form to the SA you consider to be the BCR lead.
- You may attach additional pages or annexes if there is insufficient space to complete your responses.
- You may indicate any responses or materials that is in your opinion commercially sensitive and should be kept confidential but, in any case, be aware that the relevant document will be shared among the concerned SAs and the European Data Protection Board (EDPB) which, under Article 64, has to issue its opinion on the approval draft decision of your BCRs. Requests by third parties for disclosure of such information, will, however, be handled by each supervisory authority involved in accordance with national legislation.
- The footnotes in the application form indicate the relevant provisions of the Article 47 GDPR and Working Party papers WP 256 and specific Sections of WP 74 and WP 108, which contain further clarification of the questions still valid under the framework of the GDPR.
- Once you have submitted the form, the SA you approached will circulate Part 1 of the form to all the 'concerned supervisory authorities'[2] in order to determine who should be the BCR Lead;

[1] This questionnaire takes also into account the draft standard application form for approval of Binding Corporate Rules drawn up by the ICC.

[2] Pursuant to Article 4(22)(a) and (b), a 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because the controller or processor is established on the territory of

- You will be informed by the SA you approached which SA has finally been appointed by all SAs concerned to act as BCR Lead;
- As a rule, the BCR Lead will seek the cooperation of two other SAs concerned (SAs co-reviewers) in order to assess the BCRs in the light of Article 47 and WP 256[3];
- Once revised, in accordance with Article 64 GDPR, the BCR Lead will circulate the remainder of the form including your BCRs to all the other supervisory authorities concerned in order to collect their views to be sent to European Data Protection Board (EDPB) along with the draft opinion on the BCRs.

the Member State of that supervisory authority or because "data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing". As for the BCRs approval procedure, the concerned SAs are the SAs in the countries from where the transfers are to take place as specified by the applicants or, in case of BCR-P, all SAs (since a processor established in a Member State may provide services to controllers in several – potentially all – Member States).

[3] As a rule, the BCR Lead will consult 2 co-reviewers whenever 14 Member States are concerned by transfers. Under this threshold it is possible to have one or two co-reviewers depending on the specific case and the availability of SAs.

PART 1 APPLICANT INFORMATION

Section 1: Structure and Contact Details of the Applicant and of the Group of group of undertakings, or group of enterprises engaged in a joint economic activity ('Group')

- If the Group has its headquarters in the EEA the form should be filled out and submitted by that EEA entity.
- If the Group has its headquarters outside the EEA, then the Group should appoint a Group entity located inside the EEA – preferably established in the country of the presumptive BCR Lead - as the Group member with "delegated data protection responsibilities". This is the entity which should then submit the application on behalf of the Group.
- Contact Details of the Responsible Party for Queries:
    - Please indicate a responsible party to whom queries may be addressed concerning the application.
    - This party need not be located in the EEA, although this might be advisable for practical reasons.
    - You may indicate a function rather than a specific person.

Section 2: Short description of data flows

- The applicant should also give a brief description of the scope and nature of the data flows from the EEA for which approval is sought.

Section 3: Determination of the BCRs Lead

- In accordance with Article 64 GDPR, the BCR Lead is the authority in charge of coordinating the approval of your BCRs which then could be considered to be appropriate safeguards in the countries within the EEA which you have named in your application as the origin of transfers of personal data by Group members to third countries, without requiring any specific authorisation for the use of the BCR from the other supervisory authorities concerned.
    - Before you approach one SA as the presumptive BCR Lead you should examine the factors listed in Section 1of WP 263 (still the same already enlisted in Sections 3.3 and 3.4. of WP 108). Based on these factors you should explain in Part 1.3 of your application which SA should be the BCR Lead. The SAs are not obligated to accept the choice that you make if they believe that another SA is more suitable to be BCR Lead, in particular if it would be worth for speeding up the procedure (e.g. taking into account the workload of the originally requested SA).

PART 2 BACKGROUND PAPER

Section 4: Binding Nature of the Binding Corporate Rules

- In order for the BCRs to be approved for the transfer of personal data, they must be shown to have legally binding effect both internally (between the Group entities, and on employees and subcontractors) and externally (for the benefit of individuals whose personal data is processed by the Group) in accordance with national legislation. These questions elicit the information necessary to determine if your BCRs have such binding effect.
- Your application will need to make clear that the burden of proof with regard to an alleged breach of the rules will rest with one member of the Group established on the territory of a Member State (e.g. the member at the origin of the transfer or the European headquarters

or that part of the organisation with delegated data protection responsibilities), regardless of where the claim originates.

- Regulators in some sectors (such as the financial services industry) may prohibit an entity of the Group in one country from assuming liability for another Group entity in another country. If this is the case for your application, please provide details about this situation in the subsection "Legal claims or actions" and explain any other mechanisms your Group has implemented to ensure that an aggrieved individual can obtain recourse against the Group in the EEA.

Section 5: Effectiveness

- Effectiveness (verification of compliance) may be demonstrated by a variety of mechanisms typically implemented by companies, such as a regular audit programme, corporate governance activities, compliance departments, etc. Please respond to the questions on effectiveness based on the verification mechanisms used in your group.
- You will need to confirm that you will permit the concerned SAs in the EEA to audit your compliance.

Section 6: Cooperation with SAs

- Section 6 focuses on cooperation with SAs. You have to specify how your BCRs deal with the cooperation with SAs.

Section 7: Description of Processing and Data Flows

- In order for the SAs to assess whether your BCRs provide adequate safeguards for the transfers of data in accordance with Article 47 GDPR, it is essential that you describe data flows within your Group in a complete yet understandable fashion.

Section 8: Mechanisms for Reporting and Recording Changes

- Both the SAs and the Group entities must be informed without undue delay about any changes to the BCRs. In particular, changes that significantly affect data protection compliance (e.g. will be detrimental to data subject rights), and not to mere administrative changes (unless they impact the BCRs - e.g. changes to the bindingness) must be promptly communicated to the concerned Supervisory Authorities, via the competent SA under Article 64 (i.e. BCR Lead)[4]. In this section, please describe the mechanisms your Group has implemented for reporting and recording such changes.
- The obligation to report changes applies only to the text of the BCRs themselves, and not to any supporting documentation, unless a change to such documentation would significantly affect compliance with the BCRs.

Section 9: Data Protection Safeguards

- In this Section please provide details of how your BCRs address the core data protection safeguards that are necessary to provide an adequate level of protection for the data that are transferred.

Annex 1: Copy of the Formal Binding Corporate Rules

- Please attach a copy of your BCRs. These need not necessarily be contained within one document and your BCRs may comprise a number of documents. In the latter case please clearly specify the legal relationship between these documents (e.g. general rules – more detailed rules for a specific area like HRM or CRM).

[4] See WP 155, Q 14.

- You do not need to attach all ancillary documentation at this stage, this may be submitted separately after discussions with the BCR Lead.

Standard Application for Approval of Binding Corporate Rules

PART 1: APPLICANT INFORMATION

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

Name of the Group and location of its headquarters:
Does the Group have its headquarters in the EEA? ☐ Yes ☐ No

Name and location of the applicant:
Identification number (if any):
Legal nature of the applicant (corporation, partnership, etc.):
Description of position of the applicant within the Group: (e.g. headquarters of the Group in the EEA, or, if the Group does not have its headquarters in the EEA, the member of the Group inside the EEA with delegated data protection responsibilities)
Name and/or function of contact person (note: the contact person may change, you may indicate a function rather than the name of a specific person):
Address:
Country:
Phone number: Fax: E-Mail:

EEA Member States from which BCRs will be used:

2. SHORT DESCRIPTION OF PROCESSING AND DATA FLOWS[5]

Please, indicate the following:

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

- Do the BCRs only apply to transfers from the EEA, or do they apply to all transfers between members of the group?

- Please specify from which country most of the data are transferred outside the EEA:

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

3. DETERMINATION OF THE LEAD SUPERVISORY AUTHORITY ('BCR LEAD')[6]

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

- Location of the Group's EEA Headquarters

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

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

- Country where most of the decisions in terms of the purposes and the means of the data processing are taken

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

[5] See Article 47.2. a and b and Section 4.1. WP 256.
[6] See Part. 1 WP 263.

PART 2: BACKGROUND PAPER[7]

4. BINDING NATURE OF THE BINDING CORPORATE RULES (BCRs)

INTERNAL BINDING NATURE[8]

Binding within the entities of the Group[9]

How are the BCRs made binding upon the members of the Group?

- ☐ Measures or rules that are legally binding on all members of the Group
- ☐ Contracts or intra-group agreement between the members of the Group
- ☐ Unilateral declarations or undertakings made or given by the parent company which are binding on the other members of the Group (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), please specify

Please explain how the mechanisms you indicated above are legally binding on the members of the Group in the sense that they can be enforced by other members of the Group (esp. headquarters):

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

[7] Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256, adopted on 6 February 2018.
[8] See GDPR Art. 47.1.a and 47.2.c and Section 1.2 WP 256. See, also, general considerations in Section 3.3.1. WP74 and in Section 5 WP108.
[9] See Section 5.3 WP108.

Binding upon the employees[10]
Your Group may take some or all of the following steps to ensure that the BCRs are binding on employees, but there may be other steps. Please, give details below. - Work employment contract - Collective agreements (approved by workers committee/another body) - Employees must sign or attest to have read the BCRs or related ethics guidelines in which the BCRs are incorporated - BCRs have been incorporated in relevant company policies - Other means (but the group must properly explain how the BCRs are made binding on employees) - Disciplinary sanctions for failing to comply with relevant company policies, including dismissal for violation Please provide a summary supported by extracts from policies and procedures or confidentiality agreements as appropriate to explain how the BCRs are binding upon employees.

Binding upon subcontractors processing the data[11]
What steps have you taken to require subcontractors to apply protections to the processing of personal data (e.g., through the use of obligations in your contracts with them)? Please specify:
How do such contracts or other legal acts under Union or Member State law address the consequences of non-compliance?
Please specify the sanctions imposed on subcontractors for failure to comply

[10] See Article 47.1.a and Section 1.2 WP 256 and Section 5.8 WP108.
[11] See Art. 28.3 GDPR and Section 5.10 WP108.

EXTERNALLY BINDING NATURE[12]

How are the rules binding externally for the benefit of individuals (third party beneficiary rights) or how do you intend to create such rights? For example you might have created some third party beneficiary rights in contracts or unilateral declarations[13].

Legal claim or actions
Explain how you meet the obligations according to the requirement of Articles 47.2.e, 77 and 79, 82 GDPR[14]

Please confirm that the controller established on the territory of a Member State (e.g. the European headquarters of the Group, or that part of the Group with delegated data protection responsibilities in the EEA), has made appropriate arrangements to enable itself or the member of the Group at the origin of the transfer payment of compensation for any damages resulting from the breach, by any part of the Group, of the BCRs and explain how this is ensured.
Please confirm that the burden of proof with regard to an alleged breach of the rules will rest with the member of the Group at the origin of the transfer or the European headquarters or that part of the organisation in the EEA with delegated data protection responsibilities, regardless of where the claim originates.

[12] See 47.1.b and 47.2.c and e GDPR and Section 1.3 WP 256. See also general considerations in Section 3.3.2 WP74.

[13] 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 WP 256),
- Transparency and easy access to BCRs (Art. 47.2.g and Section 6.1, Section 1.7 WP 256),
- 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),
- 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 WP 256),
- Cooperation duties with Data Protection Authority (Art. 47.2.k and l, Section 3.1 WP 256),
- Liability and jurisdiction provisions (Art. 47.2.e and f, Section 1.3, 1.4 WP 256).

Furthermore, you must be fully aware of the fact that according to civil law of some jurisdictions unilateral declarations or unilateral undertakings do not have a binding effect. In the lack of a specific legislative provision on bindingness of such declarations, only a contract with third party beneficiary clauses between the members of the Group may give proof of bindingness.

[14] See also Section 1.3. WP 256: 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).

5. EFFECTIVENESS[15]

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

Training and awareness raising (employees)

- Special training programs

- Employees are tested on BCRs and data protection

- BCRs are communicated to all employees on paper or online

- Review and approval by senior officers of the company

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

Internal complaint handling[16]

Do the BCRs contain an internal complaint handling system to enforce compliance?

Please describe the system for handling complaints:

[15] See Articles 47.2.j and 47.2.l and Art. 38.3 GDPR and Section 2.3 WP 256. See also general considerations in Section 5.2 WP74 and Section 6 WP108.

[16] See Articles 47.2.i and 12.3 GDPR and Section 2.2 WP 256. See also Section 5.3 WP74.

Verification of compliance

What verification mechanisms does your Group have in place to audit each member's compliance with your BCRs? (e.g., an audit programme, compliance programme, etc)? Please specify:

Please explain how your verification or compliance programme functions within the Group (e.g., information as to the recipients of any audit reports and their position within the structure of the Group).

Do the BCRs provide for the use of:

- Data Protection Officer? Choose by clicking here
- internal auditors? Choose by clicking here
- external auditors? Choose by clicking here
- a combination of both internal and external auditors? Choose by clicking here
- verification by an internal compliance department? Choose by clicking here

Do your BCRs mention if the verification mechanisms are clearly set out in…

- a document containing your data protection standards Choose by clicking here
- other internal procedure documents and audits? Choose by clicking here

Network of data protection officers (DPO) or appropriate staff [17]

Please confirm that a network of DPOs or appropriate staff (such as a network of privacy officers) is appointed with top management support to oversee and ensure compliance with the BCR for Processors:

Please explain how your network of DPOs or privacy officers functions:

- Internal structure:

- Role and responsibilities:

6. COOPERATION WITH SAs[18]

[17] See Section 2.4 WP 256.
[18] See Article 47.2.l GDPR and Section 3.1 WP 256 and Section 5.4 WP 74.

Please, specify how your BCRs deal with the issues of cooperation with SAs:

Do you confirm that you will permit the concerned SAs to audit your compliance? Do you confirm that the Group as a whole and each of the companies of the Group will abide by the advice of the concerned Supervisory authority relating to the interpretation and the application of your BCRs?

7. DESCRIPTION OF PROCESSING AND DATA FLOWS[19]

Please indicate the following:

- Nature of the data covered by the BCRs, e.g. HR data, and in particular, if they apply to one category of data or to more than one category

- What is the nature of the personal data being transferred?

- In broad terms where do the data flow to and from?

- What are the type of processing and the purposes for which the data covered by the BCRs are transferred to third countries and of the processing that is carried out after the transfers?

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

Do the BCRs only apply to transfers from the EEA, or do they apply to all transfers between members of the Group? Please specify:

[19] See Article 47.2.b GDPR and Section 4.1 WP 256 and Section 7 WP108.

8. MECHANISMS FOR REPORTING AND RECORDING CHANGES[20]

Please, confirm and explain how your BCRs allow for informing other parts of the Group and the concerned SAs, via the competent SA under Article 64 (i.e. the BCR Lead), of any changes to the BCRs and/or the list of BCR members (summary):

Please confirm that you have put in place a system to record any changes to your BCRs.

9. DATA PROTECTION SAFEGUARDS[21]

Please, specify with reference to your BCRs how and where the following issues are addressed with supporting documentation where appropriate:

- Transparency and fairness and lawfulness

- Purpose limitation

- Data minimisation and accuracy

- Limited storage periods

- Processing of special categories of personal data

- Security (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)

- Restrictions on onward transfers

- Other (e.g. protection of children, etc.)

[20] See Article 47.2.k GDPR and Section 5.1. WP 256.
[21] See Article 47.2.d GDPR and Section 6.1. WP 256.

10. ACCOUNTABILITY AND OTHER TOOLS[22]

-Please confirm and specify how BCR members will be responsible for and able to demonstrate compliance with the BCRs

-Please confirm that the BCR members will 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. 30.1 GDPR.

-Please confirm that data protection impact assessments will 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) and that 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)

- Please confirm and specify which appropriate technical and organisational measures will be implemented to comply with data protection principles and facilitate compliance with the requirements set up by the BCRs in practice (e.g. data protection by design and by default, GDPR Art. 25)

Please provide supporting documents where appropriate with respect to the information requested above

[22] See Section 6.1.2 WP256

ANNEX 1:
COPY OF THE FORMAL BINDING CORPORATE RULES

Please attach a copy of your BCRs. Note that this does not include any ancillary documentation that you would like to submit (e.g. specific privacy policies and rules).