# ARTICLE 29 DATA PROTECTION WORKING PARTY

**Working Document 02/2012 setting up a table with the elements and principles to be found in <u>Processor</u> Binding Corporate Rules**

**Adopted on 6 June 2012**

# INTRODUCTION

The Article 29 Working Party already developed some tools[1] to facilitate the use of Binding Corporate Rules (BCR) for Controllers ("BCR for your own data"), intended to regulate the transfers of personal data that are originally processed by the company as Controller (such as data relating to its customers, its employees, etc.).

In this paper, the Article 29 Working Party intends to develop a toolbox, describing the conditions to be met, to facilitate the use of Binding Corporate Rules (BCR) for Processors ("BCR for third party data").

BCR for Processors aim to frame international transfers of personal data that are originally processed by the company as Data Processor according to the external instructions of a Data Controllers (such as outsourcing activities).

According to the EU Directive 95/46/EC, a contract should be signed between a controller and a processor. This contract will be referred here as the "service agreement".

---

[1] See WP153 (toolbox to check all conditions to be met), WP155 (FAQs), WP 154 (Example of BCR) and WP 74 and 108 (originate papers).

| Criteria for approval of BCR | In the BCR | In the application form | BCR Processor |
|---|---|---|---|
| **1 - BINDING NATURE** | | | |
| **INTERNALLY** | | | |
| **1.1 The duty to respect the BCR** | YES | YES | The BCR must contain a clear duty for all the members of the Group and for its employees to respect the BCR. The BCR shall also expressly state that all the members of the Group and the employees shall respect the instructions regarding the data processing and the security and confidentiality measures as provided in the Service Agreement (Art. 17 Directive). |
| **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 :<br><br>i) Between the companies/entities in the group by one or more of:<br>Intra-group agreement,<br>Unilateral undertakings,<br>Internal regulatory measures,<br>Policies of the group, or<br>Other means<br><br>ii) On employees by one or more of:<br>Individual and separate agreement/undertaking with sanctions ,<br>Clause in employment contract with sanctions,<br>Internal policies with sanctions, or<br>Collective agreements with sanctions |
| **EXTERNALLY** | | | |
| **1.3 The creation of third-party beneficiary rights for data subjects, including the possibility to lodge a complaint before the competent Data Protection Authorities and before the courts (choice of jurisdiction between court of EU Processor data exporter/ EU data processor headquarters/EU member with delegated data protection responsibilities/EU Controller and if those situations are not applicable; Court of DS residence)** | YES | YES | The BCR must grant rights to data subjects to enforce the BCR 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.<br><br>The data subjects' rights shall cover the judicial remedies for any breach of the rights guaranteed and the right to receive compensation for any damage (material harm but also any distress).<br><br>Data subjects shall be entitled to lodge a complaint before the DPA or Courts competent for the EU Controller. If this is not possible for the reasons stated above, the data subject may take action before the DPA or the court competent for the EU entity of the processor at the origin of the transfer or the EU headquarters of the Processor, the EU Member with delegated data protection responsibilities of the Processor. If those situations are not applicable, the data subjects shall be entitled to lodge a complaint to the court of his place of residence. If more favourable solutions for the data subject exist according to national law, then they would be applicable.<br><br>The third party beneficiary right shall cover: Point 1.1, 1.3, 1.5, 1.7, 1.8, 2.2, 3.1, 3.2, 6.1, 6.2, 6.3 |

| Criteria for approval of BCR | In the BCR | In the application form | BCR Processor |
|---|---|---|---|
| **1.4. Responsibility towards the Controller** | YES | YES | The BCR shall be made binding toward the Controller through a specific reference to it in the Service Agreement.<br><br>Moreover, BCR must state that all data controller shall have the right to enforce the BCR against any entity for breaches they caused. Moreover, the entity referred under point 1.5 arising out of a breach of the BCR or of the Service agreement by members of the BCR for Processor established outside of EU or of a breach of the written agreement referred under 6.1.vii, by any of external sub-processor established outside of EU.<br><br>The data controllers' rights shall cover the judicial remedies and the right to receive compensation. |
| **1.5 The company accepts liability for paying compensation and to remedy breaches of the BCR.** | YES | YES | The BCR must contain a duty for the EU headquarters of the processor or the EU Member of the Processor with delegated responsibilities or the EU exporters processor (e.g. the EU contracting party with the controller) to accept responsibility for and to agree to take the necessary action to remedy the acts of other members of the BCR established outside of EU or breaches caused by external sub-processor established outside of EU and to pay compensation for any damages resulting from the violation of the BCR .<br><br>This 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 member of the group outside the EU or the external sub-processor established outside of EU.<br><br>This 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.<br><br>In case no member of the BCR Processor is established in the EU, the Headquarter of the group will take this liability (located outside of the EU). In this case, data subjects and data controller shall be entitled to lodge a complaint before the DPA or Courts of their place of residence/establishment. |
| **1.6 The company has sufficient assets.** | NO | YES | The application form must contain a confirmation that the entity that has accepted liability for the acts of other members of the BCR outside of the EU and for external sub-processor established outside of EU has sufficient assets to pay compensation for damages resulting from the breach of the BCR. |
| **1.7 The burden of proof lies with the company not the individual.** | YES | YES | BCR must state that where data subjects or Data controller can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of BCR, it will be for the member of the group that accepted liability to prove that the member of the corporate group outside of Europe or the external sub-processor was not responsible for the breach of the BCR giving rise to those damages or that no such breach took place[2].<br>If the entity that has accepted liability can prove that the member of the group outside the EU is not responsible for the act, it may discharge itself from any responsibility. |

---

[2]  See also FAQ11 of WP155 applicable to BCR for Controller.

| Criteria for approval of BCR | In the BCR | In the application form | BCR Processor |
|---|---|---|---|
| **1.8 There is easy access to BCR 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 BCR is part of the contract. BCR will be annexed to the Service Agreement or a reference to it will be made with a possibility of electronic access.<br><br>Access for Data subject : BCR shall be published on the website of the Group of processor 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 |

| **2 – EFFECTIVENESS** | | | |
|---|---|---|---|
| **2.1 The existence of a suitable training programme** | YES | YES | The BCR must state that appropriate training on the BCR will be provided to personnel that have permanent or regular access to personal data, that are involved in the collection of personal data or in the development of tools used to process personal data.<br><br>The Data Protection Authorities evaluating the BCR 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. |
| **2.2 The existence of a complaint handling process for the BCR** | YES | YES | The BCR shall contain a commitment from the Processor Group to create a specific contact point for the data subject.<br><br>All member of the BCR shall have the duty to communicate the claim or request without delay to the Controller without obligation to handle it, (except has been agreed otherwise with the Controller).<br><br>The BCR shall contain a commitment for the Processor to handle complaints from data subjects where data controller has disappeared factually or has ceased to exist in law or became insolvent.<br><br>In all cases where the processor handles complaints, these shall be dealt with by a clearly identified department or person who has an appropriate level of independence in the exercise of his/her functions.<br><br>In those cases, data subject shall be informed about :<br>- where to complain,<br>- in which form,<br>- the timescale for the reply on the complaint,<br>- consequences in case of rejection of the complaint<br>- consequences in case the complaint is considered as justified<br>- consequences if the data subject is not satisfied by the replies (right to lodge a claim before the Court/Data Protection Authority) |

| Criteria for approval of BCR | In the BCR | In the application form | BCR Processor |
|---|---|---|---|
| **2.3 The existence of an audit programme covering the BCR** | YES | YES | The BCR 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).<br><br>The BCR must state that the audit programme covers all aspects of the BCR including methods of ensuring that corrective actions will take place. Moreover, the BCR must state that the result will be communicated to the privacy officer/function and to the ultimate parent's board but also will be made accessible to the data controller.<br><br>The BCR must state that Data Protection Authorities competent for the data controller can have access to the results of the audit upon request and give them the authority/power to carry out a data protection audit themselves if required and legally possible.<br><br>Any processor or sub-processor handling the data 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 DPA.<br>The application form will contain a description of the audit system. For instance:<br>- which entity (department within the group) decides on the audit plan/programme,<br>- which entity will make the audit,<br>- time of the audit (regularly or on specific request from the appropriate Privacy function.)<br>- 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 BCR, review of the contractual terms used for the transfers out of the Group (to controllers or processors of data), corrective actions, …)<br>- which entity will receive the results of the audits. |

| Criteria for approval of BCR | In the BCR | In the application form | BCR Processor |
|---|---|---|---|
| **2.4 The creation of a network of privacy officers or appropriate staff for handling complaints and overseeing and ensuring compliance with the rules.** | YES | NO | A commitment to appoint appropriate staff (such as a network of privacy officers) with top management support to oversee and ensure compliance with the rules.<br><br>A brief description of the internal structure, role and responsibilities of the network or privacy officers or similar function created to ensure compliance with the rules. For example that the chief privacy officer advises the board of management, deals with Data Protection Authorities' investigations, annually reports on compliance, ensures compliance at a global level and that Privacy officers can be responsible for reporting major privacy issues to the chief privacy officer and for ensuring compliance at a local level. |

| | | | |
|---|---|---|---|
| **3 – COOPERATION DUTY** | | | |
| **3.1 A duty to cooperate with Data Protection Authorities** | YES | YES | The BCR shall contain a clear duty for all members of the BCR to co-operate with, to accept to be audited by the Data Protection Authorities competent for the relevant controller and to comply with the advice of Data Protection Authorities on any issue related to those rules. |
| **3.2 A duty to cooperate with the Controller** | | | The BCR 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 DPA). This shall be done in a reasonable time and to the extend reasonably possible. |

| | | | |
|---|---|---|---|
| **4 - DESCRIPTION OF PROCESSING AND DATA FLOWS** | | | |
| **4.1 A description of the transfers and material scope covered by the BCR** | YES | YES | The BCR shall contain a list of entities that are part of the BCR (see also point 6.2)<br><br>The Processor submitting a BCR shall give a general description to the DPA of the material scope of the BCR (expected nature of the data transferred, anticipated purposes and data importers/exporters in the EU and outside of the EU) |
| **4.2 A statement of the geographical scope of the BCR (nature of data, type of data subjects, countries)** | YES | YES | The BCR shall indicate that it is up to the Controller to apply the BCR to:<br>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;<br>ii)  all processing of data processed for processor activities within the group whatever the origin of the data. |

| Criteria for approval of BCR | In the BCR | In the application form | BCR Processor |
|---|---|---|---|

| **5 - MECHANISMS FOR REPORTING AND RECORDING CHANGES** | | | |
|---|---|---|---|
| **5.1 A process for updating the BCR** | YES | YES | The BCR 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 group members, to the Data Protection 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 are communicated to the new sub-processor). |
| | | | Updates to the BCR or to the list of the members of the BCR are possible without having to re-apply for an authorization providing that: |
| | | | i) An identified person keeps a fully updated list of the members of the group 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 DPA.<br>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 Data Protection Authorities.<br>iii) No transfer is made to a new member until the new member is effectively bound by the BCR and can deliver compliance.<br>iv) Any substantial changes to the BCR or to the list of members shall be reported once a year to the Data Protection Authorities granting the authorizations with a brief explanation of the reasons justifying the update. |

| Criteria for approval of BCR | In the BCR | In the application form | BCR Processor |
|---|---|---|---|

| **6 - DATA PROTECTION SAFEGUARDS** | | | |
|---|---|---|---|
| **6.1 A description of the privacy principles including the rules on transfers or onward transfers out of the EU.** | YES | YES | The BCR shall include the following principles, applicable by any member of the BCR:<br><br>i) Transparency and fairness; 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 activities in order to allow the controller to correctly inform the data subject).<br><br>ii) Purpose limitation: duty to process the personal data only on behalf of the data controller and in compliance with its instructions. If it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data controller of its inability to comply, in which case the data controller is entitled to suspend the transfer of data and/or terminate the contract;<br>On the termination of the provision of data processing services, the processors and sub-processors shall, at the choice of the data controller, return all the personal data transferred and the copies thereof to the data controller or shall destroy all the personal data and certify to the data controller that it has done so, unless legislation imposed upon them prevents it from returning or destroying all or part 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.<br><br>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:<br>- Processors and sub-processors will execute any necessary measures when asked by the Controller, in order to have the data updated, corrected or deleted.  Processor and sub-processors will inform each member to whom the data have been disclosed of any rectification, or deletion of data.<br>- 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.<br><br>iv) Security: Processors and sub-processors must comply with the security and organisational measure which at least meet the requirements of the data controller's applicable law and any existing particular measures specified in the Service Agreement.<br>Processors and sub-processors shall immediately inform the Controller of any security breach. |

| Criteria for approval of BCR | In the BCR | In the application form | BCR Processor |
|---|---|---|---|
| | | | v) Data subject Rights: Processors and sub-processors will execute any necessary measures when asked by the Controller, and communicate any useful information in order to help the Controller to comply with the duty to respect the rights of the data subjects.<br>Processor and sub-processors, will transmit to the data controller any data subject request without answering it unless he is authorised to do so.<br><br>vi) Sub-processing within the Group: data may be sub-processed by other members of the BCR only with the prior information to the Controller[3] and its prior written consent. The Service agreement will specify if a general prior consent given at the beginning of the service would be sufficient or if specific consent will be required for each new sub-processing. If a general consent is given, the controller should be informed on any intended changes concerning the addition or replacement of subcontractors 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.<br><br>vii) Onward transfers to external sub-processors: Data may subprocessed by non-members of the BCR only where the prior information to the Controller[4] and its prior written consent.. If a general consent is given, the controller should be informed on any intended changes concerning the addition or replacement of subcontractors 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.<br><br>Where the member of BCR subcontracts its obligations under the Service Agreement, with the consent of the data controller, it shall do so only by way of a written agreement with the sub-processor which provided that adequate protection is provided according to Articles 16, 17, 25 and 26 of the Directive 95/46/EC and which ensure that the external sub-processor will have to respect the same obligations as are imposed on the member of the BCR according to the Service Agreement and sections 1.3, 1.4, 3 and 6 of this WP. |

---

[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 BCR | In the BCR | In the application form | BCR Processor |
|---|---|---|---|
| **6.2 The list of entities bound by BCR** | YES | YES | BCR shall contain a list of the entities bound by the BCR. |
| **6.3 The need to be transparent where national legislation prevents the group from complying with the BCR** | YES | NO | A clear commitment that where a member of the BCR has reasons to believe that the existing or future legislation applicable to it may prevents it from fulfilling the instructions received from the data controller or its obligations under the BCR or service agreement, it will promptly notify this to the Data Controller which is entitled to suspend the transfer of data and/or terminate the contract, to the EU headquarter processor or EU member with delegated data protection responsibilities or the other relevant Privacy Officer/function, but also to the DPA competent for the controller.

Any legally binding request for disclosure of the personal data by a law enforcement authority shall be communicated to the data 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 DPA competent for the controller and the lead DPA for the BCR should be clearly informed about it. |
| **6.4 A statement about the relationship between national laws and BCR** | YES | NO | BCR shall specify the relationship between the BCR and the relevant applicable law.

The BCR 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 BCR.

In any event data shall be processed in accordance to the applicable law. |

**II. COMMITMENTS TO BE TAKEN IN THE SERVICE LEVEL AGREEMENT**

The BCR 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 that:

- BCR will be made binding 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 BCR. The Controller shall make available to the Data Subjects upon request a copy of the BCR 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 precise if data may be sub-processed inside of the Group or outside of the group and will precise if the prior consent to it expressed by the controller is general or needs to be given for each new sub-processing activities.


Done at Brussels, on 6 June 2012


*For the Working Party*
*The Chairman*
*Jacob KOHNSTAMM*