ARTICLE 29 DATA PROTECTION WORKING PARTY

00658/13/EN
WP 204

Explanatory Document on the Processor Binding Corporate Rules

Adopted on 19 April 2013

INDEX

page

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof,

has adopted the present Working Document:

1. CONTEXT

1.1. European Union rules for international data transfers

The Directive requires that data transfers outside the European Union shall be strictly framed in order to make sure that data subjects benefit from an adequate level of protection even when their data is sent outside the European Union (hereinafter "EU").

Art. 26.2 of the Directive provides that *"(…) a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection (…), where the controller adduces adequate safeguards with respect to the protection of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses*."

Consequently, when the country of the importer of data does not ensure an adequate level of protection, the Controller must provide sufficient guarantees to the data transferred, for instance by the adoption of contractual clauses.

On this basis, and in order to facilitate compliance with the Directive 95/46 of data transfers outside the EU, the European Commission adopted sets of standard contractual clauses - 2001/497/EC on 15 June 2001 and 2004/915/EC on 27 December 2004 – in order to frame transfers between Controllers; and 2010/87/EU on 5 February 2010 for transfers between Controllers and Processors.

1.2. Binding corporate rules for Controllers

Realizing the need for organisations to have a global approach to data protection, the Article 29 Working Party deemed it necessary to authorise organisations to adopt binding internal rules, the so-called binding corporate rules (hereinafter "BCR"), intended to regulate the transfers of personal data that are originally processed by the organisation as Controller within the same organisation. EU Data Protection Authorities developed a "tool box" providing guidance on what is expected in BCR[2].

[1] Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[2] See WP153, WP154 and WP155 http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/tools/index_en.htm

It is important to note on the sideline, that while standard contractual clauses are an 'out-of-the-box' solution, each set of BCR needs to be tailor-made to the particular needs of a given corporation. And while standard contractual clauses are usually signed without the need for any particular implementation, BCR is based on the organisation having a sufficiently satisfactory and robust data protection regime already in place within the group or introducing the necessary measures to ensure that the systems in place meet the BCR requirements.

Over the last few years, BCR for Controllers have proved to be more and more successful. The length of the adoption procedure has been considerably reduced due not just to the increasing experience of Data Protection Authorities and organisations but also to the mutual recognition procedure. Also, multinational organisations have constantly reaffirmed that BCR fit in the pragmatic approach they strive for with regard to compliance issues. In addition, the European Commission brought its support to BCR by including it in the draft regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, published on 25 January 2012[3].

1.3. Binding corporate rules for Processors

In 2010, the European Commission adopted a new set of standard contractual clauses for transfers between Controllers and Processors in order to answer to the expansion of processing activities and in particular the emergence of new business models for international processing of personal data. The 2010 standard contractual clauses contain specific provisions allowing, under certain conditions, the outsourcing of processing activities to sub-processors, while ensuring sufficient guarantees to personal data transferred.

Guaranteeing a continuously adequate level of protection with the use of available tools for framing international data transfers, as described above, is proving difficult, which is mainly due to the increasing number and complexity of international data transfers (resulting from e.g. Cloud computing, globalisation, data centres, social networks, etc.).

While standard contractual clauses appear to be efficient to frame non-massive transfers made by a data exporter located in the EU to a data importer located outside the EU, the outsourcing industry has been constant in its request for a new legal instrument that would allow for a global approach to data protection in the outsourcing business and officially recognize internal rules organisations may have implemented. Such new legal instrument would be efficient to frame massive transfers made by a Processor to subprocessors part of the same organisation acting on behalf and under the instructions of a Controller. Given the growing interest of industry for such a tool, the Working Party adopted in the course of 2012 a working document setting up a table with the elements and principles to be found in BCR for Processors[4] and an application form for submitting binding corporate rules for Processors[5].

---

[3] See Article 42 of the draft regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[4] See WP195, adopted on 6 June 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

[5] See the application form for approval of binding corporate rules for the transfer of personal data for processing activities, adopted on 17 September 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_application_form_en.doc

The launch of Processor binding corporate rules was confirmed by the Working Party on 5 December 2012[6].

2. DEFINITION AND LEGAL ISSUES AT STAKE

2.1. Scope of this instrument and definitions

BCR for Processors are meant to be a tool which would help frame international transfers of personal data that are originally processed by a Processor on behalf of an EU Controller and under its instructions[7], and that are sub-processed within the Processor's organisation.

Therefore, BCR for Processors shall be annexed to the Processor contract (referred to in this paper as the Service Level Agreement) which is required by Art. 17 of EU Directive 95/46 and contains notably the instructions of the Controller signed between the external Controller and the Processor. BCR for Processors should be understood as adequate safeguards provided by the Processor to the Controller (Art. 26.2 of EU Directive 95/46) allowing the latter to comply with applicable EU data protection law. The Processor's group entities shall commit to respect the principles contained in the BCR for Processors and shall be held liable vis-à-vis the Controller in case of breach of the BCR for Processors.

However, it is important to highlight the fact that although EU Data Protection Authorities assess the content of the BCR for Processors of a Processor group in order to ensure that all the requirements from the WP195 are satisfied with, the Controller remains liable of ensuring that sufficient guarantees are provided to the data transferred and processed on its behalf and under its instructions within the entities of the Processor's group.

The Working Party reminds that BCR for Processors do not aim to shift Controllers' duties to Processors. The Processors and Controllers' duties in the context of international transfers of data will remain unchanged (analogous to standard contractual clauses 2010/87/EU) but some tools will need to be adapted to the particularities of transfers within a same group of organisations (one global commitment instead of multiple contracts) and to the particularities of BCR (accountability tools such as audit, training programmes, data protection officers…).

In addition, BCR for Processors should enhance data subjects' rights by providing expressly that Processors commit to provide Controllers with the relevant information to enable them to respect their obligations towards data subjects. BCR for Processors appear to be an additional guarantee that Processors undertake to provide the relevant information to Controllers.

Finally, while a Processor will have to apply for the EU recognition of its BCR for Processors as adequate safeguards for international transfers according to the mutual recognition and cooperation procedures provided for by WP107[8], Controllers will still have to apply for national authorisations with the competent Data Protection Authorities to transfer data to the different entities of their service providers (Processors, sub-processors, data centres...) on the basis of BCR for Processors being part of the guarantees brought by Controllers

---

[6] See the press release issued on 21 December 2012, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20121221_pr_bcrs_en.pdf

[7] A third party Controller called upon an outsourcing company which will make international transfers of those data to entities of its group of companies which will act as sub-processors.

[8] See WP107, adopted on 14 April 2005, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp107_en.pdf

2.2. Transfers and onward transfers

2.2.1. Transfers within the Processor's group

Considering that according to WP195, data may be sub-processed by other members of the Processor's group only with the prior information to the Controller[9] and its prior written consent, BCR for Processors provide for transparency towards the Controller and leave the latter in control over the data processed by the entities of the Processor's group on its behalf and under its instructions.

The parties to the Service Agreement are free to decide, depending on their particular needs, if a general prior consent given by the Controller at the beginning of the service would be sufficient or if a specific consent from the Controller 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.

A Processor's organisation that have implemented BCR for Processors will not need to sign contracts to frame transfers with each of the sub-processors part of its organisation as BCR for Processors adduce safeguards to data transferred and processed on behalf and under the instructions of a Controller.

2.2.2. Onward transfers to external sub-processors

In addition to the rules set out above for the transfers within the Processor's group (transparency, consent of the Controller), a member of the Processor's group may subcontract its obligations under the Service Agreement (Art. 17 of the Directive) to an external sub-processor (outside of the group) only by way of a written agreement with the external sub-processor which provides that adequate protection is adduced according to Articles 16, 17 of Directive 95/46/EC and which ensures that the external sub-processor will have to respect the same obligations as are imposed on the member of the Processor's group according to the Service Agreement and sections 1.3, 1.4, 3 and 6 of the working document 195[10]. Moreover, to the extent that BCR for Processors do not apply to transfers to external sub-processors (outside of the group), adequate protection shall be adduced to such transfers in accordance with Articles 25 and 26 of Directive 95/46/EC.

2.3. Considerations about the binding nature of the BCR for Processors

Processors respond to the needs of their data processing activities on the basis of different legal and cultural backgrounds and different business philosophies and practices. From the experience with BCR for Controllers, it is clear that nearly every multinational organisation approaches this matter in a different way. There is, however, among others, an important element which must be present in all systems if they are to be used to adduce safeguards for the data transfers to third countries for processing activities: the binding nature of the corporate rules for Processors both internally and towards the outside world (legal enforceability of the rules).

---

[9] 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.

[10] *Op. cit*. 6

2.3.1. Binding nature of the corporate rules for Processors within the organisation[11]

A distinction can be made between the problem of compliance with the rules and the problem of their legal enforceability.

Indeed, the assessment of the "binding nature" of such corporate rules for Processors implies a common assessment of their external and internal binding nature in law.

The binding nature of the rules internally, in this respect, would imply that the members of the organisation of the Processor, as well as each employee within it, are compelled to comply with the internal rules. In that respect, relevant elements could include the existence of disciplinary sanctions in case of contravention of the rules, individual and effective information of employees, setting up special education programmes for employees and subcontractors, etc. All these elements, which are also considered at section 4, could establish why individuals within the Processor's organisation will feel obliged to comply with these rules.

With respect to the Processor's group members, it is not for the Working Party to stipulate the way in which organisations should guarantee that all the members are effectively bound or feel compelled by the rules although some examples are well known such as internal codes of conduct backed by intra group agreements[12]. But organisations must bear in mind that those applying for the approval of their BCR for Data Processors as adequate safeguards provided by the Processor to the Controller (Art. 26.2 of EU Directive 95/46) will have to demonstrate to Data Protection Authorities that such BCR for Processors are effectively binding throughout the group.

The internal binding nature of the rules must be clear and good enough to be able to guarantee compliance with the rules outside the EU, normally under the responsibility of the EU headquarters, the EU member with delegated data protection responsibilities or the EU data exporter Processor which must take any necessary measures to guarantee that any member adjust their sub-processing activities to the undertakings contained in the BCR[13].

As a matter of fact, there is in most cases an EU based member of the organisation adducing sufficient safeguards and dealing with the BCR for Processor's application before the lead data protection authority. If the headquarters of the organisation is based outside the EU, the headquarters should delegate these responsibilities to a member based in the EU, if any. It makes sense that the effective adducer of the safeguards remains responsible for the effective compliance with the rules and guarantees enforcement. However, another mechanism can be accepted, i.e. liability lying upon the EU exporter Processor. See in this regard sections 4.6 and 4.7 on liability and jurisdiction.

---

[11] The adoption of a code of conduct is a step that corporations do not take lightly because its adoption poses significant risks and even legal consequences for those organisations that breach their own code.

[12] Please note that in some Member States, only contracts are regarded as binding. You would, therefore, need to take local advice if you intended to rely on other legal means than contracts.

[13] Under international corporate law affiliates may be able to enforce codes of conduct against each other based on claims of quasi-contractual breach, misrepresentation and negligence.

2.3.2. Binding nature of the corporate rules for Processors upon external sub-processors processing the data

When the Processor subcontracts its obligations under the Service Agreement (Art. 17 of the Directive) to an external sub-processor with the consent of the Controller, it shall do so only by way of a written agreement with the sub-processor. See in this regards section 2.2.2. on onward transfers.

2.3.3. Legal enforceability of the corporate rules

2.3.3.1. Legal enforceability of the corporate rules by the data subjects (third party beneficiary rights)

Data subjects covered by the scope of the BCR for Processors must become third party beneficiaries by means of inclusion of a third party beneficiary clause within the BCR which must be given a binding effect either by unilateral undertakings (where possible under national law) or by contractual arrangements between the members of the Processor's group.

In any case, data subjects shall be entitled to enforce compliance with the rules against the Controller both by lodging a complaint before the data protection authority or before the court competent for the EU Controller as explained in section 4.6.

However, in case data subjects are not able to bring a claim against the Controller[14], they may also take action against the Processor before the data protection authority or court competent for (i) the EU headquarters of the Processor, or (ii) the EU member of the Processor's group with delegated data protection responsibilities, or (iii) the EU exporter Processor.

If this choice is not practicable (for instance, there is no Processor establishment within the EU), data subjects shall be entitled to lodge a complaint to the court of their place of residence. In any case, if more favourable solutions for a data subject exist according to national applicable law (such as it exists in consumer law or labour law), they then would be applicable.

Where in some cases the legal enforceability of a third party beneficiary clause contained in unilateral declarations does not raise any doubts, in other Member States the situation is not that clear and unilateral declarations might not be sufficient as such. Where unilateral declarations cannot be considered as granting legally enforceable third party beneficiary rights, the organisations would have to put in place the necessary contractual arrangements allowing for that. Contractual arrangements can be legally enforced under private law in all Member States[15].

The principles covered by the BCR which are to be made enforceable through the third party beneficiary rights clause are as follows:

[14] It may be the case if the 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 Controller by contract or by operation of law, in which case data subjects can enforce their rights against such entity.

[15] Nowadays it is possible to grant third party beneficiary rights in a contract in all Member States. See at this point previous experiences with standard contractual clauses and third party beneficiaries.

- Duty for the Processor to respect the BCR as well as the Controller's instructions regarding the data processing as well as the security and confidentiality measures as provided for in the Service Agreement (WP195 section 1.1);

- Creation of third-party beneficiary rights for data subjects (WP195 section 1.3);

- Processor's liability for paying compensation and to remedy breaches of the BCR (WP195 section 1.5);

- The burden of proof lies with the Processor, not data subjects (WP195 section 1.7);

- Easy access to the BCR for data subjects (WP195 section 1.8);

- Existence of a complaint handling process for the BCR (WP195 section 2.2);

- Duty to cooperate with Data Protection Authorities (WP195 section 3.1) and with the Controller (WP195 section 3.2);

- Privacy principles (WP195 section 6.1);

- List of Processor entities bound by the BCR (WP195 section 6.2);

- Transparency where national legislation prevents the Processor from complying with the BCR (WP195 section 6.3).

Contractual arrangements do not need to be complex or long. They are only instruments to trigger third party beneficiary rights for the individuals in those countries where there are doubts that unilateral declarations may achieve a similar result. In some cases, this could be achieved with the addition of a simple clause to other contracts in place between the members of the Processor's group.

2.3.3.2. Legal enforceability of the corporate rules by the Controller

BCR for Processors are a safeguard for international transfers provided by a Processor to its client (Controller) and it is the Controller that is primarily liable towards Data Protection Authorities and data subjects for ensuring that personal data transferred outside the EU are protected. As such, BCR for Processors shall be made binding toward the Controller through a specific reference to it in the Service Agreement.

In addition to this and in order for the BCR for Processors to be unambiguously linked to the Service Agreement signed with each client (Controller), it is important to make sure in the Service Agreement that:

- the Controller shall commit that if the transfer involves special categories of data, data subjects have been informed or will be informed before the transfer that their data could be transmitted to a third country not providing adequate protection;

- the Controller shall also commit to inform data subjects about the existence of Processors based outside of EU and of the BCR for Processors. The Controller shall make available to data subjects upon request a copy of the BCR for Processors and of the Service Agreement (without any sensitive and confidential commercial information);

- clear confidentiality and security measures are described or referred to with an electronic link;

- a clear description of the instructions and the data processing is provided;

- the Service Agreement will precise if data may be sub-processed inside of the Processor's group or outside of its group and will specify if the prior consent to it expressed by the Controller is general or needs to be given for each new sub-processing activities.

The Data Protection Authorities evaluating the BCR may not ask to be provided with such Service Agreement but in all cases a summary supported by extracts from this agreement shall be provided in the application form to explain how the BCR for Processors are made enforceable by Controllers.

Moreover, the BCR will include a third party beneficiary right clause for the benefit of the Controller in order to ensure that it will be entitled to enforce the BCR, which shall cover the judicial remedies and the right to receive compensation, against any member of the Processor's group.

2.3.3.3. Legal enforceability of the corporate rules by the Data Protection Authorities

If a Processor submits an application for the EU recognition of its BCR for Processors as adequate safeguards provided by the Processor to the Controller (Art. 26.2 of EU Directive 95/46), it is clear that the Processor's group binds itself *vis-à-vis* the EU data Protection Authorities to respect the safeguards adduced (in this case the BCR for Processors). Nevertheless, it will be the task of the Controller to ask for the required national authorisation for the international transfer of data, which is to be clearly distinguished from the recognition of BCR as adducing sufficient safeguards to data transfers. BCR for Processors already "approved" (and not "authorised") at EU level will be referred by the Controller as the appropriate safeguards proposed for the international transfers.

Insofar as Article 28 of EU Directive 95/46 provides for that Data Protection Authorities "*(...) are responsible for monitoring the application within their territory of the provisions adopted by the Member States pursuant to this Directive"*, it means that they have the duty, among others, to supervise transfers and assess the guarantees to transfer data outside of the EU.

In order to achieve such responsibilities, Data Protection Authorities are endowed with investigative powers, effective powers of intervention on their territory, as well as the power to engage in legal proceedings; such powers might be used against a Processor that would not comply with the BCR.

In addition, a breach of the BCR for Processors by a member of the Processor's group (or by the entire group) might lead to the withdrawal of the authorisation of the concerned transfer granted to the Controller on the basis of the BCR for Processors. Such withdrawal would not be retroactive.

2.3.4. Mandatory requirements of national legislation applicable to the members of the organisation

The BCR should contain a clear provision indicating that where a member of the Processor's group 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 BCR or the Service Agreement, it will promptly notify this to:

- the Controller which is entitled to suspend the data transfer and/or terminate the Service Agreement; and

- the EU Processor headquarters or EU member with delegated data protection responsibilities or the relevant Processor's privacy officer/function; and

- the Data Protection Authority competent for the Controller.

In addition, the Processor shall communicate any legally binding request for disclosure of the personal data by a law enforcement authority 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 Data Protection Authority competent for the Controller and the lead Data Protection Authority for the BCR for Processors should be clearly informed about it.

However, it will be necessary to ensure that transfers of personal data to a law enforcement authority are based on legal grounds according to the applicable law, insofar as the BCR for Processors' requirements from WP195 Section 6.3 only create an information process (see above) that does not legitimate transfers *per se*. In the case of a conflict of laws, one shall refer to the international treaties and agreements applicable to such matter.

3. SUBSTANTIAL CONTENT OF THE BINDING CORPORATE RULES FOR PROCESSORS

3.1. Substantial content and level of detail

The data protection principles from the Directive need to be developed and detailed in the BCR for Processors so that they practically and realistically fit with the processing activities carried out by the organisation in the third countries and can be understood and effectively applied by those having data protection responsibilities within the organisation.

Section 6 of the WP195 gives more explanation about this content.

The description of the transfers in the BCR can only be general, but more precise information about the particular transfers of a particular Controller will have to be given in the framework of the national authorisation procedure with the competent Data Protection Authorities. The level of detail in the BCR must be sufficient so as to allow the Data Protection Authorities to assess that the safeguards adduced to data processing and sub-processing carried out in third countries by a member of the Processor's group are adequate.

3.2. Updates to the BCR

The Article 29 Working Party acknowledges that organisations are mutating entities whose members and practices may change frequently, so that the transfers taking place on behalf and under the instructions of Controllers and, as matter of course, the rules contained in the BCR cannot continuously correspond to the reality at the time the recognition as an adequate protection was given.

Thus, BCR for Processors can be modified (for instance to take into account modifications of the regulatory environment or the organisational 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 manner that the latter 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 for Processors or to the list of the members of the BCR for Processors are possible without having to re-apply before the Data Protection Authorities provided 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 Controller, data subjects and Data Protection Authorities.

ii) This person will keep track of and record any updates to the rules and provide the necessary information systematically to the Controller and upon request to Data Protection Authorities.

iii) No transfer is made to a new member until the new member is effectively bound by the BCR for Processors and can deliver compliance.

iv) Any substantial changes to the BCR for Processors or to the list of members shall be reported once a year to the Data Protection Authorities granting the authorizations of transfers to the Controller(s) with a brief explanation of the reasons justifying the update.

Updating the rules should be understood in the sense that working procedures may change and the rules would need to be adapted to such changing environments.

4. DELIVERING COMPLIANCE AND GUARANTEEING ENFORCEMENT

In addition to those rules dealing with substantial data protection principles, any binding corporate rules for Processors must also contain:

4.1. Provisions guaranteeing a good level of compliance

The rules are expected to set up a system which guarantees awareness and implementation of the rules both inside and outside the European Union. The issuing by the headquarters of internal privacy policies must be regarded only as a first step in the process of adducing sufficient safeguards within the meaning of Article 26 (2) of the Directive. The applicant organisation must also be able to demonstrate that such a policy is known, understood and

effectively applied throughout the group by the employees who have received appropriate training and have the relevant information (including the BCR) always available, for example via the intranet. The organisation should appoint the appropriate staff, with top-management support, to oversee and ensure compliance.

4.2. Audits

The rules must provide for data protection audits and/or external supervision by internal or external accredited auditors on a regular basis with direct reporting to the privacy officer/function and ultimate parent's board as well as being made accessible upon request to the Controller[16].

BCR for Processors must also state that Data Protection Authorities competent for the Controller can have access to the results of these audits upon request and give them the authority/power to carry out a data protection audit themselves if required and legally possible. This is most likely to be the case where the audits foreseen in the previous paragraph were not available for whatever reasons, they failed to contain relevant information necessary for a normal follow-up of the approval delivered by Data Protection Authorities or the urgency of the situation would advocate in favour of a direct participation of the Data Protection Authority competent for the Controller.

Such audits would take place in accordance with the relevant laws and regulations governing the Data Protection Authorities' investigatory powers, without any prejudice to the inspection powers of each Data Protection Authority. In any case, they will take place with full respect to confidentiality and trade secrets and would be narrowly limited to ascertaining compliance with the binding corporate rules.

In addition, BCR for Processors shall state that any processor or sub-processor handling the data of a particular Controller will, at the request of that Controller, allow their data processing facilities to be audited in relation to the processing activities of that Controller. Such audit 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 Controller, where applicable, in agreement with its competent Data Protection 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/program;

- 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 BCR for Processors, review of the contractual

[16] The content of these audits must be comprehensive and elaborate in any case about some particulars already identified in this working document, such as the existence of onward transfers on the basis of standard contractual clauses (see section 2.2.2.) or the decisions taken as regards mandatory requirements under national law which may create conflicts with the binding corporate rules (see section 3.3.3.).

terms used for the transfers out of the Processor's group (to Controllers or Processors), corrective actions, …);

- Which entity will receive the results of the audits.

4.3. Complaint handling

BCR for Processors shall contain a commitment from the Processor group to create a specific contact point for the data subject.

All members of the BCR for Processors shall only have the duty to communicate the claim or request without delay to the Controller without obligation to handle it (except if it has been agreed otherwise with the Controller).

It is only where the Controller has disappeared factually or has ceased to exist in law or became insolvent that the Processor will have to handle any such communication.

Where the Processor handles complaints (when it is agreed with the Controller or the Controller disappeared or ceased to exist), 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.

In those cases, data subject shall be informed about:

- Where to complain;

- In which form;

- The timescale 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/Data Protection Authorities).

4.4. The duty of co-operation with the Controller

BCR for Processors shall expressly state that all the members of the Group and the employees shall respect the Controller's instructions regarding the data processing and the security and confidentiality measures as provided in the Service Agreement (Art. 17 Directive).

The rules shall also 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 investigations or inquires from Data Protection Authorities). This shall be done in a reasonable time and to the extent reasonably possible.

4.5. The duty of co-operation with Data Protection Authorities

As outlined in WP 12, one of the most important elements for assessing the adequacy of a self-regulatory system is the level of support and help available to individual data subjects: *"A key requirement of an adequate and effective data protection system is that an individual faced with a problem regarding his personal data is not left alone, but is given some institutional support allowing his/her difficulties to be addressed"*.

This is indeed an important element of the BCR for Processors: the rules must contain clear duties for all members of the Processors' group to cooperate with the Data Protection Authorities competent for the relevant Controller so individuals can benefit from the institutional support mentioned in the working document 12.

There must also be an unambiguous undertaking that the organisation as a whole and any of its members separately will abide by the advice of the competent Data Protection Authority on any issues related to the interpretation and application of these BCR for Processors.

Before issuing any advice the competent Data Protection Authority may seek the views of the organisation, the data subjects concerned, the relevant Controller and those Data Protection Authorities which may be associated as a result of the co-ordinated procedure foreseen in this working document[17]. The advice of the authority may be made public.

In addition to any relevant provision at national level, a serious and/or persistent refusal by the organisation to co-operate or to comply with the advice of the competent Data Protection Authority may result in the suspension or the withdrawal of the authorization transfer granted to the relevant Controller(s), either by the Data Protection Authority itself or the competent authority under national law empowered to do so. A direct consequence of such suspension or withdrawal will require the relevant Controller(s) to find another way to provide adequate protection to the data transferred, for instance by signing the Standard contractual clauses 2010/87/UE and to re-apply for these transfers before the competent Data Protection Authorities in accordance with the national applicable legislation.

4.6. Liability

4.6.1. General right to obtain redress and where appropriate compensation

The rules should indicate that the third party beneficiary rights provided to the data subject and the right of redress provided to the Controller should cover the judicial remedies and the right to receive compensation for any damage (for the data subject, it should cover the material harm but also any distress).

As a complement to this general right, the rules must also contain provisions on liability and jurisdiction aimed at facilitating its practical exercise.

4.6.2. Rules on liability

4.6.2.1. Rules on liability for data subjects

As third party beneficiary, data subjects are entitled to enforce the BCR against the members of the Processors' group which have breached the BCR.

[17] See chapter 5.

Moreover, the BCR for Processors shall identify which member of the group among (i) the EU headquarters or (ii) the EU member of the Processor with delegated data protection responsibilities or (iii) the EU exporter Processor (e.g., the EU contracting party with the Controller) that will accept responsibility for and agree to take the necessary action to remedy the acts of other members of the organisation established outside the EU (when they have breached the BCR or the Service Agreement) or breaches of the written contract (referred under 2.2.2.) caused by external sub-processors established outside of EU and, where appropriate, to pay compensation for any damages caused. When the organisation chooses the third option (EU exporter Processor), it shall provide explanation to the lead Data Protection Authority why it cannot have an entity which is liable for the whole group.

Instead of the member of the group outside the EU or the external sub-processor established outside of EU who breached the BRC, the identified corporate member will accept liability as if itself had committed the violation in the Member State in which it is based.

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.

In case no member of the organisation is established in the EU, the headquarters of the group, located outside of the EU, will take this liability.

4.6.2.2. Rules on liability for the Controller

BCR for Processors must state that all Controllers shall have the right to enforce the BCR for Processors against any member of the Processor's group for breaches it caused. The Controller should also have the power to enforce the written agreement (referred under 2.2.2) against any external subprocessor at the origin of the breach.

In addition to this, in case the breach is caused by a non-EU Processor's entity or by an external non-EU subprocessor, the Controller shall have the right to enforce the BCR for Processors against the Processor's entity that accepted to bear liability[18] for paying compensation and to remedy breaches of the BCR, of the Service Agreement or of the written agreements signed with the external subprocessors.

The organisation will make the commitment in its BCR for Processors' application form that the entity that has accepted liability for the acts of other members of the BCR for Processors outside of the EU and for external sub-processors established outside of EU has sufficient assets to pay those compensation for damages.

4.6.2.3. Rules on the burden of proof

BCR for Processors must also state that where data subjects or the Controller can demonstrate that they have suffered damages and establish facts which show it is likely that the damage has occurred because of the breach of the BCR for Processors (or the Service agreement or the written contracts referred under 2.2.2) , it will be for the member of the group that has accepted liability to prove that the member of the organisation outside of EU or the external sub-processor was not responsible for this breach giving rise to those damages or that no such breach took place.

[18] The EU headquarters of the Processor, or the EU Member of the Processor with delegated data protection responsibilities or the EU exporter Processor (see WP195 section 1.5)

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.

4.7. Rule on jurisdiction

As explained above in chapter 4.6.2., the organisation must also accept that data subjects would be entitled to take action against the organisation in case they are not able to bring a claim against the Controller[19], as well as to choose the jurisdiction (Data Protection Authority or Court):

a) before the competent Data Protection Authorities, or

b) in the jurisdiction of the EU Processor member that is at the origin of the transfer, or

c) in the jurisdiction of the European Processor headquarters, or

d) in the jurisdiction of the European member of the Processor with delegated data protection responsibilities, or

e) in case no member of the organisation is established in the EU, data subjects and the Controller shall be entitled to lodge a complaint before the Data Protection Authorities or Courts of their place of residence/establishment. If the data subject or the Controller resides/is established outside of the EU and brings a claim before a non-EU Court, the competent EU Data Protection Authorities should be informed of the existence of such litigation procedure and its outcome.

Assuming the proper functioning of the system which implies a good level of compliance throughout the group, regular audits, efficient complaint handling, co-operation with Data Protection Authorities, etc. the involvement of the courts seems unlikely, but in any case cannot be excluded. Having said that, only experience with these instruments will tell us if such forecast is right.

The relevant principles and rules on jurisdiction contained both in the Directive and in national laws will duly apply.

4.8. Transparency

Organisations which implement BCR for Processors must be in a position to demonstrate that data subjects have an easy access to all the commitments made under the BCR that they are entitled to enforce as third party beneficiaries. In that respect, BCR for Processors shall be published on the website of the organisation in a way easily accessible to data subjects or at least a document including all (and not a summary of) the information relating to third-party beneficiary rights as listed in chapter 2.3.3.1.

As regards to the Controller, the Service Agreement will ensure that the BCR for Processors is part of the contract. BCR for Processors will be annexed to the Service Agreement or a reference to it will be made with a possibility of electronic access.

[19] It may be the case if the 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 Controller by contract or by operation of law, in which case data subjects can enforce their rights against such entity.

5. CONCLUSION

The Working Party believes that the guidance provided in this document may facilitate the application of Article 26 (2) of the Directive in the case of BCR for Processors. It should also lead to a certain degree of simplification for multinational organisations routinely processing and exchanging personal data on a world-wide basis on behalf of Controllers.

The content of this working document should not be regarded as the final word of the Article 29 Working Party on this issue but as a solid first step to highlight the possibility to use BCR for Processors on the basis of a self-regulatory approach and co-operation among the authorities, without prejudice to the possibility to use other tools for the transfer of personal data abroad such as the standard contractual clauses or the Safe Harbor principles where applicable.

Further input from interested circles and experts on the basis of the experience obtained with the use of this working document is welcomed. The Working Party might decide to revisit this issue in the light of experience.

Done at Brussels, 19/04/2013

For the Working Party

The Chairman

Jacob Kohnstamm