10 January 2023

EBF_045974

EBF response to the European Data Protection Board's consultation on the draft Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)

1. General comments

The European Banking Federation (EBF) welcomes the opportunity to respond to the EDPB's draft Recommendations on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (BCR-C). **Certainty** in **international data transfers** and the mechanisms available is a priority for our members, particularly in light of the Court of Justice of the European Union's (CJEU) so called Schrems II ruling.

As a result, we would first like to draw attention to the **implementation modalities** for **organisations** which already have **BCR-Cs in place,** and which will have to update them.

For an efficient and smooth update of their BCR-Cs, and to ensure legal certainty, it is necessary for those organisations to have clear guidance, in particular on the following aspects:

- Details on the **time frame to comply** with the new BCR-C recommendations. In our view, organisations should have at least six months from the publication of the BCR-C to update their current BCR-Cs and comply with the new rules.
- Ensure that companies can **communicate** their **updated BCR-C to the competent authority in a flexible manner,** without having to complete a new application form once more (for example, companies could submit a version with track changes to the competent authority).
- Make sure that the updated BCR-Cs are sent to the competent authority for information, without going through a new validation process. This will enable companies to implement the changes without waiting for a decision of the authority. Indeed, the delay to obtain such a decision may be long given the backlog present

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

in Data Protection Authorities (DPAs). The authority would still be able to challenge the companies concerned ex-post.

Secondly, while a large part of the Recommendations draw from the WP256 version, there are changes which should be considered, for example on data subjects rights. Effective protection of personal data requires the strengthening and setting out the rights of data subjects. In the guidance on BCR-C as presented it is mentioned that data subjects have to be informed on every change that has been made in a BCR-C. Most of the controllers **provide information and fulfil the requirements on transparency via their privacy statement**. We therefore question whether providing information on every change in a BCR-C, would be helpful in strengthening the rights of data subject or if this overload of information would not be working against these principles.

Detailed comments follow.

2. Detailed comments

Section	Proposed Recommendation	Comments
Introduction		
Paragraph 5	"Hence, the obligations set out in BCR-C apply in relation to entities within the same Group acting as controllers and to entities acting as 'internal' processors."	Even though this was already mentioned in the WP 29 guidance, we suggest to specify what is meant by "internal processors" as in the first sentence of the paragraph, it is mentioned that the BCR-C is suitable for transfers from controllers to other controllers or processors.
	"Indeed, the obligations set forth in BCR-C apply to entities of the Group receiving personal data as ('internal') processors to the extent that this does not lead to a contradiction with the	We would recommend including an example of this to further understand the situations where there could be a

	contract or other legal act entered into under Article 28(3) GDPR (i.e., the processors members of the Group processing on behalf of controllers members of the Group should primarily abide by this contract)."	contradiction with the contract or other legal act entered into under Art. 28(3).
Paragraph 13	"The EDPB expects all BCR-C holders to bring their BCR-C in line with the requirements set out below. This includes BCR-C that have been approved before the publication of these Recommendations. Such changes will have to be done in compliance with the commitments taken in their BCR-C in accordance with Section 5.1 below."	Does this require to send an updated version to the BCR lead? We suggest to specify in the explanation which part of this **applies to already approved BCR-Cs and new BCR-C's.** For example, in the general instructions for applicants, the third bullet notes that: *Please fill out all entries of Part I of the application form and submit the form to the SA you consider to be the BCR-C Lead. As soon as a decision on the BCR Lead has been made (see WP263), the BCR Lead will determine when it will invite you to fill out and submit Part II of the application form including its Annexes.* For the already approved BCR-Cs, this is already known. We also recommend to **include a timeframe** for concluding this process. Groups of companies that already rely on approved BCR-Cs, will need to update their BCR-Cs and underlying procedures once the final version of the Recommendations are adopted and, in that process, conduct a gap analysis to identify the changes. Therefore, a timeframe that takes into consideration these steps, is needed.

1.3.1 Creation of third-party beneficiary rights that are enforceable by data subjects	"Duty to inform the data subjects about any update of the BCR-C and of the list of BCR members (see Section 8.1 below);"	This appears to be a new requirement. While we understand the aim of providing transparency, to inform data subjects of any update to the BCR-C would be a big challenge and might not help data subjects in improving their position since the information requirements are mostly been done via the privacy statements. A challenge would also be if data subjects do not have a form of electronic communication in place.
1.3.2 - Right to judicial remedies, redress and compensation for data subjects	"The BCR members accept that data subjects may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) GDPR (see Articles 77 – 82 GDPR). The BCR members should make sure that all those rights are covered by the third-party beneficiary clause of the BCR-C, for example, by making reference to the clauses, sections, and/or parts of the BCR-C where those rights are regulated, or by listing them in the said third-party beneficiary clause."	While this seems to be a new requirement, it is already included in the GDPR; we therefore question whether it should be included in the BCR-C.
1.5 The Liable BCR member(s) has sufficient assets	"The application form should contain a confirmation that the Liable BCR member(s) has sufficient assets, or has made appropriate arrangements to enable itself to pay compensation for damages resulting from a breach of the BCR-C. Such confirmation should be renewed at the occasion of every annual update (see Section 8.1 below)."	We would recommend including examples of what is meant by the term "sufficient assets."
1.7 -Easy access to the	"Furthermore, the BCR-C must contain the commitment that data subjects commitment that data subjects will be provided at least with the description of the scope of the BCR-C (see Section	Instead of the current guidance – which states that it must be easily accessible for data subjects – it is now in addition to other information provided to the data

BCR-C for data subjects	2 below), the clause relating to the Group's liability (see Section 1.4 above), the clauses relating to the data protection principles (see Section 5.1.1 below), to the lawfulness of the processing (see Section 5.1.2 below), to security and personal data breach notifications (see Section 5.1.3 below), to restrictions on onward transfers (see Section 5.1.4 below), and the clauses relating to the rights of the data subjects (see Section 5.2 below). This information should be up-to-date, and presented to data subjects in a clear, intelligible, and transparent way. This information should be provided in full, hence a summary hereof will not be sufficient."	subjects. We question whether all this information would be relevant and easily understandable.
2.1 Description of the material scope of the BCR-C	"As to the data subjects covered, BCR-C will apply to all data subjects whose personal data are transferred within the scope of the BCR-C from an entity under the scope of application of Chapter V GDPR. Therefore, the scope of the BCR-C may, in particular, not be limited to "EEA citizens or EEA residents".	The expansion of the scope of requirements also to non-EU citizens risks putting additional burdens on the data controllers. Since more countries outside of Europe are implementing privacy regulations, these provisions may lead to conflicting rules which could result in confusion for data subjects and would be difficult to implement.
2.2 – List of the BCR members, and description of the geographical	"The BCR-C shall specify the structure and contact details of the Group and of each of its BCR members (contact details of the BCR members – such as address and company registration number, where available – should be inserted in the list of BCR members that is part of the BCR-C, for example an annex thereof, that has to be published along with the BCR-C). …"	We question the proportionality of such a measure regarding the contract details in relation to the objective pursued. The result is a cumbersome provision for low-added value.

scope of the BCR-C	"The BCR-C should indicate that they at least apply to all personal data transferred to BCR members outside the EEA, and onward transfers to other BCR members outside the EEA."	In the former guidance, a controller had a choice whether onward transfers were in scope: *The BCRs should indicate if they apply to: i) All personal data transferred from the European Union within the group OR, ii) All processing of personal data within the group.* We would suggest maintaining this choice in the updated BCRs.
3.1 – Suitable training programme	"Training should cover, among others, procedures of managing requests for access to personal data by public authorities."	This puts forward an obligation to for additional mandatory content to be included on the training programme, which does not follow the GDPR or any other guidance. It would be helpful if the reason this is necessary is explained or is supported by examples.
3.2 Complaint handling process for the BCR-C	"An internal complaint handling process must be set up in the BCR-C to ensure that any data subject should be able to exercise their rights and complain about any BCR member."	We would recommend clarifying the intention of this paragraph. We assume that organisations need to set up a complaint handling process.
3.3 – Audit programme covering the BCR-C	"The audit frequency envisaged should be specified in the BCR-C. (…)"	Looking at the recommendations, we think that an existing GDPR-audit system can meet the needs of this section. Therefore, there is no need to put additional requirements on this topic.
3.3 Audit programme	"Since SAs are already bound by an obligation of confidentiality in the course of exercising their public (…) restricting the duty of all BCR members to communicate the results of the audit(s)	We have some concerns on the new provision regarding confidentiality (no possibility to restrict the duty of BCR members to communicate the audit results to the SAs); national law protecting confidential information, trade

covering the BCR-C	to the SAs on grounds of confidentiality, e.g., related to the protection of business secrets."	secrets, banking secrecy etc. should be taken into account.
3.4 Creation of a network of data protection officers (DPOs) or appropriate staff for monitoring compliance with the BCR-C	"The BCR-C should specify that the DPO or other privacy professionals may be directly contacted. The BCR-C should include a commitment to publish their contact details."	We would specify that it is the commitment to publish DPO and privacy professionals contact details, not that the contact details themselves will be included.
5.1.2 – Lawfulness of processing	"The BCR-C should contain an exhaustive list of all legal basis for processing which the BCR members intend to rely on."	In the current text, specifically the mention of an "exhaustive list," i.e., the request to list every relevant legal basis for processing including local laws, with the BCR members intend to rely on, is not proportionate. We think that the mention of the relevant GDPR articles and a general description of the national regulation can meet the same aim as the recommendation.
5.1.3 – Security and personal data breach notifications	"Without undue delay to data subjects, where the personal data breach is likely to result in a high risk to their rights and freedoms."	It is important to take into account national measures which may impact these provisions.

5.4.2 Obligations of the data importer in case of government access requests	"In any case, the BCR-C should state that transfers of personal data by a BCR member to any public authority cannot be massive, disproportionate and indiscriminate in a manner …"	The determination of "beyond what is necessary in a democratic society" is in our opinion very difficult.

ENDS

For more information:
Liga Semane
Policy Adviser – Data & Innovation
l.semane@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu