bitkom

EDPB Recommendations 1/2022the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)

Bitkom Position Paper

At a glance

EDPB Guidelines 01/2022 (BCR)

Status quo

The GDPR provides for the use of binding corporate rules (BCR) by a group of undertakings, or a group of enterprises engaged in a joint economic activity for transfers of personal data in the sense of Article 44 GDPR. In 2018, the Article 29 Working Party (WP29) adopted guidelines and principles to be found in BCR in order to reflect the requirements referring to BCR. While the European Data Protection Board (EDPB) endorsed the former Guidelines, the EDPB has now developed new Recommendations for BCR that will repeal and replace the former WP29 Guidelines.

Bitkom evaluation

Bitkom generally welcomes the EDPBs work towards a harmonized and comprehensive framework to help implement the GDPRs rules. BCRs are an important instrument for many companies to achieve legal certainty and compliance when transferring personal data to thirds countries within their group. The EDPBs recommendations would greatly benefit from some clarifications and should take the implications for companies more into account.

Most important

Additional requirements

We suggest confirming more clearly that all obligations of the GDPR, including the obligations regarding international transfers of personal data, must be interpreted in accordance with the principle of proportionality, and that this includes the recognition of the individual circumstances and whether such circumstances are likely to entail a threat to the rights and freedoms of the data subjects as introduced by Article 24(1) GDPR which confirms such concept to be applicable to all obligations in the GDPR including Art. 44 – 46 GDPR. Additional requirements that go beyond what the GDPR is requiring the companies to do should therefore be amended.

Limit bureaucracy, not extend it

Assessments for international data transfers and the process to get BCRs approved are already very extensive. Nevertheless, the EDPB Recommendations suggest even more, additional bureaucratic requirements that go beyond what Art. 47 GDPR requires. To achieve a practical, functioning implementation of the rules and keeping international data transfers alive, these additional requirements should be reconsidered.

48%

One in two companies (48 percent) exchanges data with external service providers outside the EU, one in four (25 percent) with business partners there, and 12 percent with other Group units. (Bitkom Research)

Bitkom Position

Bitkom welcomes the opportunity to provide feedback regarding the European Data Protection Board's 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).

Clear, proportionate and stable rules for the international transfer of personal data are vital for EU-headquartered companies exporting goods and services. This is especially true for all companies that are already using BCRs as a transfer mechanism.

We welcome that the EDPB´s new Guidelines aim at simplifying the application form, and the reduction in duplication between the application form and the referential. However, the EPDB should provide clarification on the impact of current (not yet approved) applications, and whether these will need to be resubmitted (presumably causing further delays).

We also believe that these draft recommendations can turn BCR-C into a less flexible legal instrument and would therefore like to offer suggestions for amendments.

While we firmly agree that the recommendations should address the need to adapt the existing guidelines for BCR-C to the new standards for international data transfers following the "Schrems II" judgment of the European Court of Justice in July 2020, we believe it will provide a more effective framework for controllers if recommendations focus on outcomes and actionable rights for the data subjects, rather than creating detailed rules that can be very demanding to implement and have no evident real benefit for individuals. With these objectives in mind, we urge the EDPB to review the recommendations considering the following observations:

Proportionality and risk based approach

In our view, the following general aspect need special attention: The EDPB should more expressly communicate the GDPR risk based model in the recommendations document. The responsibilities in these recommendations are beyond what should be required of organisations.

Existing framework and additional requirements

All companies that have already agreed to BCRs should not have to go through the approval process again. According to No. 13 on page 5 of the Recommendations, this is probably not intended. Nevertheless, adapting the existing BCRs also presents companies with practical challenges. For one thing, updates of existing documents (BCR approval documents are usually very extensive) will always mean an additional and renewed effort. Considering the existing pressure and efforts that companies need to undertake to establish BCRs and other methods to secure international data

transfers, additional efforts should only then be mandated when absolutely necessary. All companies that opted for the additional effort to use BCRs and go through the approval process should not now be required to go through even more paper work and documentation than they already have (relying on the existing Guidelines of the WP29 and the GDPR rules).

Practical issues when amending BCRs

The Guideline requires that most of the information that previously had to be provided in the application is now to be included in the wording of the BCR (see page 16 above on Annex 1. That requirement in addition to the new requirements leads to a great deal of additional work. Furthermore, coordinating updates with the competent supervisory authority is also time-consuming or takes a very long time due to their capacity constraints. Sometimes companies have to wait for a year or more for feedback on updates to their BCRs.

Going beyond the GDPR´s requirements

While Article 46 of the GDPR requires that BCRs provide "appropriate safeguards" in the third country, the EDPB's recommendation requires a 1:1 mapping of the GDPR in the BCRs. In some cases, there is even the explicit requirement that the BCRs must reflect the requirements "in the same way as ...provided in the GDPR" Part of the current BCR process is to stipulate explicitly the need for compliance with the GDPR. For the group´s companies included in the BCRs, the organizations already conduct central risk assessments to ensure that there are no regulations in the third country that conflict with the BCRs and that a comparable level of data protection exists. The measures necessary has been increased additionally to comply with the ruling of CJEU Schrems II. However, due to the large number of data transfers, it is not possible, practical or reasonable for organizations to conduct an additional in-depth security audit or an audit of every intra-company transfer (see page 39 and 10 of the Guidelines). The agreement of the BCRs, which ensure an appropriate level of protection, should suffice for this purpose. The respective paragraph should therefore be amended and the in depth audit of every transfer deleted.

In many places, a level of detail is also required in the BCR recommendations that goes far beyond the GDPR, for example, with regards to the frequency of training (Part 3, 3.1). Additionally, the Guidelines require the elements of the short-BCR to be published be set out in detail in the BCR wording (Part 3, 1.7). The provision in Art. 47 GDPR would not have been necessary if the entire GDPR were to be transferred to BCRs "in the same way".

In principle requirements and wording set out on page 10 and in Part 3, 5.4.1 on assessing local laws and practices should be aligned as much as possible with the requirements in Article 14 of the standard contractual clauses for the transfer of personal data to third countries (SCC). In particular differences in the wording between the requirements in the SCC and the recommendations (e.g. “...in particular criminal law enforcement...”, page 10; Claus 14 (b) (i) vs.

5.4.1 (i)) could lead to legal uncertainties about whether there are different levels of assessment as regards SCC and BCR-C.

Given the very extensive protections offered by the BCRs themselves (e.g. the requirements of para. 5.4.2, the accountability framework etc.) it should be the case that, in the overwhelming majority of situations, the transfers can proceed without supplementary measures above the BCRs. Additional clarifications regarding the Transfer Impact Assessments, the required level of detail and the practical implementations would therefore be helpful and we suggest the EDPB include additional information in the Guidelines.

Organizations transferring personal data under BCR-C data will have to comply with the European General Data Protection Regulation (GDPR). As result, organizations that use BCR-C to transfer personal data need to be careful in determining how data can be share, who can access to it and how to protect the security of these data with appropriate security measures in accordance with the GDPR.

The GDPR is an excellent example of principles-based regulation, rather than rules-based regulation. GDPR regulatory strategy gave flexibility by focusing on the objectives to be achieved, while supplementing this approach with guidance or even prescription as to the minimum standards necessary on limited instances.

There are strong indicators that the draft recommendations by the EDPB is a departure from the current BCR-C guidance and the GDPR itself (which do not impose such a complex system of detailed rules as the draft recommendations do).

The accountability principle of Article 5.2 GDPR and the responsibility of the controller of Article 24 GDPR were specially intended to ensure controllers are responsible for compliance with the GDPR and able to demonstrate such compliance. These obligations also apply to data transfers since they are a form of data processing in themselves.

In addition, the GDPR was intended to lessen administrative burden. However, we have pressing concerns that some of the new added requirements included in the draft recommendations would counter that intention. We included some examples below included in the draft recommendations that would have tremendous practical and cost implications, add administrative burden, and will not increase the protection of data subjects:

Duty to inform the data subjects about any update of the BCR-C and of the list of BCR members (see Section 1.3.1 draft recommendations);

Annual renewal of the confirmation that the liable BCR member(s) has sufficient assets, or has made appropriate arrangements to enable itself to pay compensation for damages (see Section 1.5 draft recommendations);

BCR-C shall specify the structure and contact details of the group and of each of its BCR members, including contact details of the BCR members such as address and company registration number (see Section 2.2 draft recommendations);

The audit frequency should be specified in the BCR-C and if audits will be carried out by external auditors, the BCR-C should specify the conditions under which such auditors may be entrusted (see section 3.3 the draft recommendations)

To the extent that current BCR-C practices have not deprived individuals of the substance of the right to data protection, we do not see the need for the above specific legal norms.

Also, we note that some of these recommendations can be at the risk of going further than other transfer legal mechanisms such as Standard Contractual Clauses (SCCs) which offer equal robust protection to data subjects.

Information to be provided

There are strong indicators that some of the elements of the draft recommendations could lead to misunderstandings and could even have a significant negative impact on how average data subjects interpret and comprehend information on the processing activities related to their personal data. In particular, article 5 (1) GDPR provides for the right of data subjects to be informed. Most organizations acting as controllers have undertaken extensive efforts to ensure their privacy notices are clear, the words and sentences are simple, the information is easy to understand and, more importantly, information is provided considering the context in which controllers are collecting personal data. We have concerns about additional and decontextualized technical information (such as the descriptions required under sections 1.7 or 5.1.2 draft recommendations), which could harm comprehension and the ability for data subjects to understand the intended meaning of the BCR-C specific updates. Individuals may even draw the inaccurate conclusions from it.

In addition, considering the broad scope of activities that fall under a set of BCR- C, information to be provided is likely to be less granular and detailed than a privacy notice (as required under article 13 and 14 of the GDPR). This is because it is unlikely to anticipate all these specific details when outlining the BCR-C. In this regard, BCR-C should be understood as setting out a framework for transfers to enable similar transfers which would be further explained in accordance with the right to be informed as established in the GDPR.

Finally, controllers should have room for maneuver to select lawful basis on case-by-case basis, considering all the specifics surrounding each data transfer. And we believe that privacy notices are again the best legal instruments to include contextual and detailed information on the lawful basis for processing, rather than BCR-C.

Limit bureaucracy, not extend it

In addition, bureaucratic requirements are also established to a greater extent, which are not in line with the binding requirements of Art. 47 GDPR. For instance, the requirement for the Intra Group Agreement to be signed at board level (Appl. Form Part 2 Sec. 5) is not required by the GDPR and also, the annual confirmation of sufficient assets (Part 3, 1.5) to the authority also goes beyond the legal text.

Right to Appeal

The requirement to comply with SA decisions (para. 4.1) should acknowledge the right to appeal.

Data Breach Notification

It is disproportionate and overly burdensome to require all BCR Members to notify the Liable BCR Member of all personal data breaches, regardless of severity (para. 5.1.3). This should be subject to the same risk threshold as SA reporting (noting, of course, that all processors would be required to notify any personal data breaches to the relevant controller).

SA Change Notification

Para. 8.1 now requires notification of modifications to BCRs that would either possibly be detrimental to the level of protection or significantly affect them to be made in advance to the lead SA. We suggest this process should be clarified to make clear under what circumstances the BCR Members are permitted to proceed with the modifications without express confirmation from the lead SA that no new approval is required.

Training Materials Development

We note the new requirement (para. 3.1) that training materials should be "developed to a sufficiently elaborate degree" before the BCRs are approved. However, given the current length of time for BCR approval (and the changes that are frequently required during the process), it would be helpful to acknowledge that these materials can be submitted at the end of the application process.

Physical Address Listing

We would question the need for a physical address for complaints (para. 3.2). Additionally, whereas previously the practical steps needed to be included in the application form, they now need to be included in the BCRs themselves. This seems unnecessary to include in the BCRs where such information is provided as part of the complaints handling process. Also, for data subjects it might be much more logical and helpful to get detailed information in the complaint handling process itself.

Contractor Terminology

The use of the term “contractors” in para. 5.3 is confusing, as it suggests Article 28 would apply to individual contractors (i.e. personnel). We suggest this only refer to processors.

DPO Conflict of Interests

Given that the GDPR requires controllers to seek the advice of the DPO when carrying out DPIAs, it is unclear why the BCR-C must specify that DPOs should not be in charge of DPIAs if this would create a conflict of interest in para. 3.4. The same query applies to audits in para 3.3. This would seem to contradict the overall requirement under GDPR that the DPO’s tasks and duties should not result in a conflict of interest.

We therefore advocate to provide clarification on the intention and rationale behind the prohibition to have data protection impact assessments carried out by the Data Protection Officers, or by extension, its office and/or assistants. The current section 3.4 creates uncertainty since the GDPR explicitly provides in relation to data protection impact assessments, for the early involvement of the DPO and it specifies that the controller shall seek the advice of the DPO when carrying out such impact assessments.

SA Confidentiality Obligations

Although all SAs are subject to a confidentiality obligation, we note that a number of Member States’ freedom of information laws may override the confidentiality obligation. We suggest starting a dialogue to evaluate possible conflicts in this regard and provide more legal certainty for controllers and SAs.

Auditor Appointment Terms

In para. 3.3, we suggest that it is not necessary for the BCRs to set out the conditions on which an external auditor may be entrusted, beyond requiring them to be accredited (which is already included in 3.3) and independent.

Keeping the benefits of BCRs alive

In addition, groups that have agreed BCRs for their companies and coordinated them with the supervisory authority should actually benefit from simplifications in the transfer of data within the group. Thus, in this case, the exchange of personal data should be possible without the need to conclude additional Joint Responsibility Agreement or Commissioned Processing Agreement.

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Publisher
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact
Rebekka Weiß, LL.M. | Head of Trust & Security | r.weiss@bitkom.org

Responsible Bitkom-Working Group
WG Data Protection