bitkom

Position Paper

February 2026

Recommendations on the Application for Approval and on the elements and principles to be found in BCR-P (Art. 47 GDPR)

Summary

Bitkom welcomes the EDPB's Recommendations 1/2026 on Binding Corporate Rules for Processors (BCR-P), which streamline approvals for intra-group processor transfers, but highlights concern on scope limitations, audit/transparency burdens, TIA requirements, and BCR change notifications that create operational inefficiencies without enhancing GDPR protections.

These recommendations strike a balance between robust safeguards and digital industry realities, enhancing BCR-P usability while maintaining data protection standards and avoiding duplication with other GDPR provisions or documentation mechanisms, such as Data Processing Agreements.

Scope of the BCR- P and scope of approval decision (1.2, 1.4)

Bitkom welcomes most updates in the EDPB’s BCR-P Recommendations but recommends clarification on Sections 1.2 and 1.4 of the introduction. These sections restrict BCR-P to intra-group processor-to-sub-processor transfers originating from EEA-based group entities subject to GDPR, excluding direct transfers from external EEA controllers to third-country group processors—which require separate Article 46 tools, such as SCCs.

This limited scope conflicts with long-standing regulatory practice from the UK ICO and WP29 (Article 29 Working Party), which permitted such direct transfers, and thus eliminates practical BCR-P utility for many organizations. This discrepancy in interpretation between the UK and the EDPB may unnecessarily strain the recognition of BCRs outside Europe (as the UK does with European BCRs through its UK BCR Addendum). Bitkom notes that this change in interpretation may also slow down the process of EU transfer mechanisms being recognized by other countries around the world (some jurisdictions are considering following the UK's approach by accepting addendums to EU existing BCRs).

This mandatory EEA routing adds an unnecessary "extra step" that neither enhances data security nor the rights of EEA residents, particularly in cloud environments where group members access data simultaneously across locations. Controller-processor contracts already reference BCR-P, certifying group-wide GDPR-equivalent safeguards (e.g., binding commitments, audits, liability), rendering processor location irrelevant. Consequently, regardless of their location, processors are legally and contractually obligated to provide the same level of data protection equivalent to that mandated within the EU[1]. Additionally, the BCR-P is binding and enforceable by the external controller against any BCR member, as specified in the processing agreement (Section 1.3.2 of the recommendations).

In light of the above, external controllers might be more inclined to select SSCs over BCR-P as their preferred method for transferring data between processor members under the processing agreement, which could make BCR-P a less appealing choice.

Bitkom recommends that the EDPB treat approved BCR-P as conferring adequate protection status under Article 45 GDPR principles for third-country group processors, enabling direct transfers without additional tools.

Responsibility towards the controller (1.3.2)

It remains unclear which BCR-P components should be included in the processing agreement, particularly regarding business secrets, confidential information (including personal data), and processors serving multiple clients.

Complaint handling process for the BCR - P (3.2)

Bitkom recommends that the BCR-P require group members to inform the complainant about any actions taken without undue delay, and in any case within one month, via a clearly designated, appropriately independent department or individual. If the request is complex or if there are multiple requests, this timeframe may be extended by up to two months, provided the complainant is notified of the extension. Further clarification is needed on who is responsible for responding to complaints from individuals. Data processors manage requests from data subjects as specified in the contract with the

[1] Also see EDPB's Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s).

controller and in accordance with Articles 12, 28(3)(e) GDPR and section 6 of the Recommendations.

Frequently, the controller does not inform the processor whether the complaint has been fully or partially resolved, or if it has been rejected. In such cases, the processor may lack clarity about the outcome and any follow-up measures that might be required. This can create uncertainty regarding the processor's compliance status and the appropriate steps to further support the controller in handling data subjects' complaints.

While data subjects are encouraged to use the point(s) of contact indicated, this is not mandatory. Bitkom recommends that the EDPB avoids encouraging complaints through any channel, as this may cause confusion for data subjects and the entity regarding whether requests are submitted to the entity as a data controller or as a data processor. Furthermore, processors should not be required to respond to requests sent to unofficial or incorrect addresses.

Bitkom further recommends eliminating the reference to email addresses and phone numbers. At minimum, if the data processor maintains an internet website, data subject requests shall be submitted through its website, such as through a webform. This approach would simplify the process for the data subject to submit their request to the entity acting as either a data controller or a data processor.

Audit and Oversight requirements (3.3.1, 3.3.2)

Bitkom recommends that BCR-P audit results should only be shared upon customer request and only under strict confidentiality safeguards to protect sensitive internal information and personal data. WP257 rev.0 requires controllers and third-party auditors to maintain confidentiality. It is also unclear what data processing facilities for audit must be submitted by the processor to the controller, or to another independent auditor mandated by the controller. Similarly, organizations with approved BCR-P should be permitted to adopt alternative audit models, including the appointment of jointly selected independent auditors, and relevant certifications held by the members of the Group, as is the case with SCCs[2].

TIA requirements for controllers (8.1)

Bitkom highlights the operational challenges of requiring TIAs "in agreement with the controller," particularly for processors serving numerous clients, and seeks clarification of this ambiguous term to ensure workable implementation. These assessments have a

[2] See section 8.9(d) Documentation and compliance: «The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer."

highly standardized nature and are typically purchased from law firms, so they should suffice given industry practice.

The expectation that controllers receive follow-ups on TIAs via the data exporter would also add unnecessary administrative layers without necessarily contributing additional protection, as outlined above.

Section 8.1 adopts a strict approach without considering the specific circumstances of the transfer or previous experience in the respective country, as is the case with the Standard Contractual Clauses (SCCs). Bitkom recommends that the EDPB explicitly allow a BCR-P data exporter to consider at least the same elements of a transfer-specific risk assessment as provided under Sections 33 and 43 of Recommendations 01/2020 and under Footnote 12, Clause 14 of the SCCs

Termination (9)

Bitkom recommends that the BCR-P allow the transfer of personal data processed on behalf of the controller to other members of the group who are effectively bound by the BCR-P. For the reasons outlined above, Bitkom suggests the following amendment to Section 9:

The BCR-P should specify that a data importer which ceases to be bound by the BCR-P should, at the choice of the controller, delete or return all personal data processed on behalf of the controller, delete existing copies, and demonstrate that it has done so. Where possible, the data importer may transfer the personal data to another BCR - member who shall continue the processing on behalf of the controller. If, pursuant to the controller's choice, the data is kept by the importer, the importer should inform the controller and guarantee the confidentiality of the data and that it will not actively process the transferred data further. This is without prejudice to any requirements under applicable third-country law applying to the data importer that prohibits return or destruction of the personal data. In such case, the data importer should guarantee that it will apply the same level of protection as that granted by the BCR-P and process the data only for as long as required under that third-country law.

BCR Change Notification (11)

Bitkom highlights the disproportionate burden of requiring notification to controllers for any BCR change, given that BCRs are publicly available and can be consulted at any time; only important or material change to the BCR-C should trigger mandatory notification, as minor updates like adding/removing group legal entities have limited impact on processing activities. Non-substantial changes for the controller or the Supervisory Authority include reformatting of the BCR-P documentation and corrections of misspellings and stylistic/ grammatical flaws.

The requirement to inform controllers of changes "affecting processing conditions" in time to modify or terminate contracts adds unnecessary bureaucracy, particularly since sub-processor changes are already covered by existing Data Processing Agreement mechanisms, thereby creating redundancy, as outlined above.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Elena Kouremenou | Policy Officer for Data Protection
P +49 30 27576-425 | e.kouremenou@bitkom.org

Responsible Bitkom committee
WG Data Protection

This publication is intended to provide general, non-binding information. The contents reflect the view within Bitkom at the time of publication. Although the information has been prepared with the utmost care, no claims can be made as to its factual accuracy, completeness and/or currency; in particular, this publication cannot take the specific circumstances of individual cases into account. Utilising this information is therefore sole responsibility of the reader. Any liability is excluded. All rights, including the reproduction of extracts, are held by Bitkom.