ITI response to the EDPB consultation on Recommendations 1/2026 on the Application for Approval and on the elements and principles to be found in Processor Binding Corporate Rules (Art. 47 GDPR)

March 2, 2026

The Information Technology Industry Council (ITI) is the premier voice, advocate, and thought leader for the global information and communication technology (ICT) industry. Our member companies include the world's leading innovation companies, with headquarters worldwide and value chains distributed around the globe. ITI member companies represent the breadth of the technology ecosystem, including semiconductor and computer hardware and software companies, network equipment manufacturers and suppliers, cybersecurity providers, and leading Internet services and consumer technology companies.

Together with our members, ITI works with governments, regulators, and stakeholders around the world to strengthen and align approaches towards data protection and privacy that safeguard individual rights and promote innovation.

I. Overview

ITI appreciates the opportunity to respond to the European Data Protection Board (EDPB) consultation on Recommendations for Processor Binding Corporate Rules (BCR-P). BCRs are widely considered the gold standard for cross-border transfers of EU personal data to non-adequate jurisdictions and many ITI members either rely on or are in the process of obtaining approval for BCR-P.

ITI recognizes the goal to update the existing BCR-P referential to ensure it remains clear, relevant and in line with regulatory requirements. While we appreciate the EDPB's efforts to clarify and promote BCR-P adoption, we are concerned about certain proposed changes that could introduce unnecessary compliance burdens and limit the BCR-P's overall effectiveness as a key enabler of trusted cross-border data flows. We would welcome the opportunity to discuss the below points in greater detail.

II. Detailed comments

Section 1.2 Scope of BCR-P

ITI's primary concern relates to the Recommendations' assertion that BCR-Ps cannot be relied upon for direct transfers from an external EEA Controller to a non-EEA BCR-P group entity, and that such transfers would instead require a separate transfer tool. This represents a significant departure

from current industry best practice and the long-standing official position of EU data protection authorities.[1]

The BCR-P has consistently been recognized as a legal tool designed to regulate transfers made by a Processor to Sub-Processors part of the same organization acting on behalf and under the instructions of an external Controller.[2] The BCR-P represents a comprehensive data privacy management program that the corporate group implements consistently across all of its operations and corporate entities globally. As these rules are binding in nature, they obligate all members and employees to ensure that every aspect of data processing and sub-processing complies with the GDPR requirements.[3] Consequently, regardless of location, they are legally and contractually obligated to provide the same level of data protection equivalent to that mandated within the EU.

Unlike Standard Contractual Clauses (SCCs), BCRs undergo strict review by EU Data Protection Authorities and EDPB approval. The BCR-P therefore represents a single straightforward recognized data transfer mechanism to enable international transfers. It is contradictory to suggest that BCR-Ps approved by EDPB are insufficient to legitimize an initial transfer and that SCCs—which do not require EDPB's approval—are required. This position undermines the perceived value of the BCR-P framework. Requiring an external Controller to, for example, now sign Standard Contractual Clauses (SCCs) for the initial Controller-to-Processor transfer while relying on BCR-P for subsequent sub-processing creates a redundant "double-transfer" requirement.

Not only would this create unnecessary and burdensome paperwork for companies to implement new agreements or amend existing ones, but it would also undermine the perceived value of the BCR-P framework as a comprehensive transfer mechanism and run counter to the EU's drive for simplification. Utilizing BCR-P to cover all relevant transfers, as is the case today, significantly simplifies the process for all parties involved without lowering data protection standards.

Organizations considering BCR-P should not be disadvantaged and put in a less competitive position than those relying on other data transfers mechanisms, such as SCCs. As a result, Controllers may prefer using SSCs instead of BCR-P as the transfer mechanism among BCR members in the processing agreement.

---

[1] See Article 29 Working Party's WP257 rev01 endorsed by EDPB on 25 May 2018, page 2: "It should be recalled that BCR-P apply to data received from a controller established in the EU which is not a member of the group and then processed by the group members as processors and/or sub processors."

[2] The EDPB's Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s) requires that "the controller's documented instructions with respect to initial or onward transfers of personal data are to be passed down along the processing chain". Additionally, section 1.3.2 of the recommendation's states that "the BCR-P should include a statement that the BCR-P will be made binding toward and enforceable for the Controller against any BCR member through a specific reference to them in the processing agreement which shall comply with article 28 of the GDPR."

[3] The BCR-P requires every member of the Group and their employees to follow and comply with the instructions of the external controller, as stated in the processing agreement (in accordance with Article 28(3)), ensuring that the transferred personal data is processed on behalf and under the instructions of the external controller throughout the processing chain. They are also required to implement appropriate technical and organizational measures to ensure the security and confidentiality of the personal data in accordance with the processing agreement, GDPR Articles 28, 29, and 32, and the Intercompany Agreement (Section 5.1.1).

We also note that the EDPB's proposed change in position runs counter to the UK Information Commissioner's Office stance that UK BCR-P's cover this type of transfer. The differing interpretations between the UK's ICO and the EDPB could create unnecessary challenges for recognizing BCRs outside of the European Union, similar to how the ICO uses its UK BCR Addendum for EU BCRs. Additionally, this shift in interpretation may delay the acceptance of EU transfer mechanisms in other countries, as some jurisdictions are considering adopting the UK's approach by accepting addendums to existing EU BCRs.

For the reasons noted above, we suggest the following amendment to Section 1.2:

> *BCR-P apply to data that will be processed by members of the Group covered by the geographical scope of the GDPR pursuant to article 3 GDPR acting as processors on behalf of a controller that is not a member of the Group ("external controller"). This includes a direct transfer from an external controller covered by the geographical scope of the GDPR to a processor of a BCR-P Group in a third country and transfers or onward transfers by a processor of a BCR-P Group to a~~, and which are then transferred by such processors to and processed by~~ Group member~~s~~ as a sub-processor~~s~~ in a third country.~~ies, including any onward transfers to other BCR members in third countries.~~ Hence, the obligations set out in BCR-P apply to entities within the same Group acting as processors and to entities acting as 'internal' sub processors, whether the data is received directly or indirectly from an external controller covered by the geographical scope of the GDPR. ~~BCR-P are, however, not suitable to cover a direct transfer from an external controller5 covered by the geographical scope of the GDPR to one of the processors members of the BCR-P Group in third countries. For such a transfer, a different transfer tool under Article 46 is required instead.~~*

Section 1.5 Update of existing BCR-P

ITI is concerned that Clause 17, as currently drafted, could be read to require companies currently undergoing the BCR-P approval process to redraft their entire draft BCR-P documentation. This would further delay an already extensive approval process which often takes many years to complete, and further reduce incentives for wider BCR adoption.

Elements and principles to be found in BCR-P

1.3.2 Responsibility toward the controller

The BCR-P must either be attached to the processing agreement or referenced within it, with electronic access to the BCR-P provided. This requirement is not sufficiently clear because the BCR-P includes business secrets and other confidential information, including personal data. The Recommendations should clarify that making the public version accessible on the corporate group's website fulfills the requirement to provide the BCR-P to the Controller.

3.2 Complaint handling process for the BCR-P

While providing a means for individuals to contact the BCR member is clearly important, providing an email address can actually be detrimental. Publicly posted email addresses become the target of spammers for purposes not related to data protection, which creates an additional burden on the

DPO and privacy offices. The part of the organization tasked with addressing data subject requests should instead be empowered to implement appropriate contact tools that allow for traceability and follow-up (for instance, a ticketing system). This allows for a higher degree of responsiveness than an email address and organizations should be able to provide web forms as an acceptable option. Additionally, we caution the EDPB against creating a de facto incentive for individuals to lodge complaints via any available channel. This raises uncertainty and can become an impediment to an efficient and timely response.

The BCR-P must require group members to inform the complainant about actions taken without undue delay, and at the latest within one month, through a clearly designated department or individual who operates with sufficient independence. If the request is complex or numerous, this period may be extended by up to two additional months, provided the complainant is notified of the extension.

We would welcome additional clarity around the responsibility for responding to complaints from individuals. Under Article 28(3)(e) GDPR, a Processor is not responsible for complying with a request, but it shall "*assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights*." Additionally, Section 6 of the Recommendations state that "*any BCR member acting as data importer shall promptly notify the data exporter and, where instructed to do so by the controller or at the controller's order as communicated by the exporter, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller or, at the controller's instruction, by the exporter*."

In most cases, the controller does not inform the Processor whether a complaint has been fully or partially accepted or rejected. The Processor also does not receive information regarding the outcome of a rejection or when a complaint is determined to be valid.

3.3.1 Audit programme covering the BCR-P

Regarding the requirement that BCR audit results be communicated to Controllers, we would like the Recommendations to make clear that audit results should only be shared upon customer request and only under strict confidentiality safeguards to protect sensitive internal information.

3.3.2 Audit by the controller and the exporter

Regarding the requirement to allow Controllers, Data Exporters, or their chosen independent auditor to conduct direct audits, it should also be made clear in the Recommendations that organizations with BCR-P are 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.[4] When getting a certification, for instance, the

[4] *S*ee section 8.9(d) Documentation and compliance of SCCs. "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."

certification requirements might overlap with BCR-P requirements and duplicating an audit process is an unnecessary strain on resources. The elements and principles should recognize the ability to meet requirements for multiple mechanisms on a single review mechanism.

WP257 rev.01 requires Controllers and third-party auditors to maintain confidentiality.[5] We also recommend 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.

For the reasons noted above, we suggest the following amendment to Section 3.3.2:

> *Any member of the Group processing the personal data on behalf of a controller will accept, at the request of that controller, at reasonable intervals or if there are indications of non-compliance, to submit their data processing facilities for audit by the controller of the processing activities relating to that controller, or by another independent auditor mandated by the controller at their cost. Audits shall be carried out with reasonable notice and the audit plan should be provided.*
>
> *Audits can also be carried out by the exporter or an independent auditor selected by the exporter. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller on grounds of confidentiality, e.g. related to the protection of business secrets. In deciding on an audit, the controller may take into account relevant certifications held by the members of the Group.*

8.1 Local laws and practices affecting compliance with the BCR-P

The requirement that Transfer Impact Assessments (TIAs), also known as local country assessments, be carried out "in agreement with the controller" should be modified. As drafted, it raises operational and practical challenges for Processors serving large numbers of Controllers, especially given the highly standardized nature of these assessments which are typically purchased from law firms, and the ambiguity of what "in agreement" entails.

We also have concerns regarding the expectation that Controllers should receive relevant follow-ups on TIAs via the Data Exporter (i.e., the obligation for Data Exporters to "inform the controller in case they identify...developments"). This requirement would add unnecessary administrative layers without necessarily contributing additional protection, in line with the reasoning above.

Section 8.1. appears to be taking a strict approach without considering the specific circumstances of the transfer or previous experience in the respective country, as is the case with Standard Contractual Clauses (SCC), for instance.[6] We recommend that the EDPB explicitly allows a BCR-P data exporter to consider at least the same elements of a transfer specific risk assessment as

[5] See Page 12 of Article 29 Working Party's WP 257 rev.01

[6] The SCCs acknowledge under footnote 12 of clause 14 (Local laws and practices affecting compliance with the Clauses) that, when assessing the different limitations and safeguards provided under the recipient country laws, the exporter should account for the specific circumstances of the transfer.

provided under Sections 33 and 43 of EDPB's Recommendations 01/2020 and under Footnote 12, Clause 14 of the SCCs.

9 Termination

The BCR-P should allow personal data transfers to group members bound by the BCR-P. As such, we suggest the amendment below 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 it has done so. Where possible, the data importer may transfer the personal data to other BCR members to continue processing the personal data on behalf of the controller. If, pursuant to the controller's choice, the data are kept by the importer, the importer should inform the controller and guarantee the confidentiality of data and that it will not actively process the data transferred anymore. This is without prejudice to any requirements under third country law applicable to the data importer prohibiting return or destruction of the personal data. In that case, the data importer should guarantee to apply the same level of protection granted by the BCR-P and to process the data only for as long as required under that third country law.*

11 Mechanisms for Reporting and Recording Changes: Process for updating the BCR-P

Regarding the requirement to notify Controllers of any change to the BCRs, we would like to propose that only significant changes should necessitate mandatory notification. Given that BCRs are publicly available and can be consulted by Controllers at any time, requiring notification for minor changes, such as the addition or removal of group legal entities, would impose a disproportionate administrative burden relative to the limited impact such changes have on customers' 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.

In addition, we do not agree with the requirement to inform Controllers of BCR changes affecting processing conditions in time for them to object to the change or terminate the contract before the modification is made, noting that the Recommendations also include Sub-Processor changes in this category (i.e., as "affecting processing conditions"), which is redundant and adds unnecessary bureaucratic steps as Sub-Processor notifications are already covered through existing Data Processing Agreement mechanisms.