30 St Mary Axe
London EC3A 8EP
TEL +44 (0)20 7220 5700

2 March 2026

European Data Protection Board (EDPB)
Rue Montoyer 30
1000 Brussels

Re: Considerations for 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)

Dear Ms. Talus, dear Ms. Vereecken and Mr. Le Grand, dear Members of the European Data Protection Board,

The Centre for Information Leadership (CIPL) welcomes the opportunity to provide comments on the draft Recommendations 1/2026 on the Application for Approval and on the elements and principles to be found in Processor Binding Corporate Rules (BCR-Ps) under Article 47 of the General Data Protection Regulation (the Recommendations).

CIPL has long supported Binding Corporate Rules (BCR) as an innovative, comprehensive, and accountability-based data transfer mechanism, developed collaboratively by regulators and industry, and explicitly recognised by Article 47 GDPR. BCR enable effective, responsible, and transparent global data processing within corporate groups and are widely regarded as the gold standard for privacy governance. In particular, in the context of BCR-Ps, processors that have obtained BCR approval see clear business value in being able to demonstrate to clients that they utilize a BCR-based data protection and security program in respect of processing client data.

Against this background, CIPL wishes to raise one fundamental concern regarding the draft Recommendations. This concern goes to the core purpose, viability, and future relevance of BCR-Ps and gives rise to a number of serious practical and policy consequences.

Key concern: exclusion of direct transfers to BCR-P members in third countries

CIPL's central concern relates to the statement in Section 1.2 of the draft Recommendations that: "BCR-P are … not suitable to cover a direct transfer from an external controller covered by the geographical scope of the GDPR to one of the processor members of the BCR-P Group in third countries."

This statement represents a significant departure from long-standing regulatory interpretations and established practice, including prior guidance developed by the Article 29 Working Party and applied by several leading supervisory authorities.[1] It fundamentally alters how BCR-Ps have been understood, implemented, and relied upon for many years by both processors and controllers.

[1] Article 29 Data Protection Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, Adopted on 28 November 2017 (As last Revised and Adopted on 6 February 2018).

As drafted, this language removes a core and widely used function of BCR-Ps to be used as a lawful mechanism for initial data transfers between EU controllers and foreign processors. In this way, organisations are forced to rely on alternative transfer mechanisms (most commonly Standard Contractual Clauses (SCCs)), even where a group has already invested substantial time, resources, and regulatory engagement to implement robust, regulator-approved BCR-Ps.

No explanation is provided as to the benefit or risk reduction achieved by this change. Instead, it introduces significant additional administrative burden and legal complexity without enhancing protection for individuals.

Consequences of the proposed approach

1. Increased bureaucracy without additional protection

The practical workaround implied by the draft Recommendations, requiring EU controllers to contract exclusively with an EU-based group entity, followed by onward transfers within the group, does not deliver additional substantive protection. The same processing operations, technical safeguards, and internal governance arrangements remain unchanged. What increases is paperwork, contractual layering, and compliance friction.

For organisations that have embedded BCR-Ps into their acquisition strategies, operating models, and global contracting frameworks, this change would require a fundamental re-engineering of long-established structures, creating confusion, duplication, and operational risk, particularly in complex processing chains involving hundreds of entities.

2. Disregard for the reality of commercial contracts and data flows in third party service provision

Importantly, this change does not reflect the realities of commercial contracting, nor the complexities of data flows between controllers and processors in the context of all kinds of IT, technology and outsourcing environments. In a modern data ecosystem, data does not move in a simple, linear fashion from point A to point B, but rather is accessed and processed by multiple entities, both on the controller side and processor side, as a part of the provision of services. This was one of the reasons why legal experts and industry practitioners repeatedly called for changes to the SCCs to make them more flexible, modular and practical for the reality of complex data flows.

It is not the role of Supervisory Authorities to dictate the commercial realities of data flows or to prescribe contracting practices within the modern data processing ecosystem. Rather, the ultimate goal of the Supervisory Authorities should be to see to ensure that the data transfer mechanisms provide effective protection for personal data. The BCR inherently achieve this by default.

3. Lost opportunity to evolve BCR resulting in undermined accountability and incentivising worse outcomes

BCR were designed as an accountability mechanism: a legally binding, regulator-approved corporate code that demonstrates the existence of a comprehensive data protection management programme across an entire group, including clear allocation of responsibility and liability through identified BCR members.

BCR-Ps are fundamentally different from, and in many respects stronger than, SCCs. While SCCs are bilateral contracts designed for linear data transfers, BCR-Ps embed accountability and governance across complex, multi-entity processing environments. By steering organisations away from BCR-Ps and toward SCCs, the draft Recommendations risk favouring mechanisms that offer weaker structural accountability and rely primarily on commercial enforcement rather than integrated privacy governance.

Moreover, excessive administrative burden creates the wrong incentives. When compliance becomes disproportionately complex, organisations are more likely to seek workarounds that are less transparent and potentially less protective, ultimately increasing risks to individuals.

With the introduction of the GDPR, there was a genuine opportunity to evolve BCR into a robust certification or a trust-mark mechanism grounded in demonstrable accountability. This evolution could have made BCR more suited to the demands of digital transformation and the realities of an interconnected digital ecosystem. Such changes might have included alleviating the burden of regulatory approval by introducing third party accountability agents or enforceable self-declaration, similar to the EU-US Data Privacy Framework.

We recall the pioneering efforts by the DPAs and the EU Commission, and industry stakeholders in creating BCR as an accountability-based concept. We encourage renewed focus and leadership from the EDPB on this matter to further develop BCRs in this direction. CIPL has repeatedly called for a more strategic and future proof approach to BCR in our work and papers.[2] However, this opportunity seems to have been overlooked and, perhaps, lost.

4. Increased prescriptiveness and administrative burden

The draft Recommendations also introduce additional prescriptive obligations relating to audits, training, record-keeping, and communications. These requirements significantly increase administrative workload without clear evidence of added protection, particularly where organisations already operate mature, regulator-approved BCR programmes.

Specifically, the Recommendations introduce:

---

[2] CIPL, The GDPR's First Six Years Positive Impacts, Remaining Implementation Challenges, and Recommendations for Improvement, May 2024, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/gdpr_six_years_on_cipl_may24.pdf; Bojana Bellamy, International data transfers: Time to rethink binding corporate rules, March 8, 2023, available at https://iapp.org/news/a/international-data-transfers-time-to-be-bold-and-rethink-binding-corporate-rules; CIPL, CIPL response to the EDPB 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), January 10, 2023, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_edpb_draft_recommendations_1-2022_10_january_2023.pdf; CIPL, GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges, May 31, 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_report_on_gdpr_one_year_in_-_practitioners_take_stock_of_the_benefits_and_challenges.pdf; CIPL, Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms, April 12, 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.

- **Communication of audit results to controllers**: Audit results should only be shared upon customer request and under strict confidentiality safeguards to protect sensitive internal information.
- **Direct audit rights for controllers, data exporters, or their chosen auditors**: Organisations should be permitted to adopt alternative audit models, such as jointly selected independent auditors, rather than mandating direct audits.
- **Transfer Impact Assessments (TIAs) "in agreement with the Controller"**: For processors serving large numbers of controllers, this is operationally impractical, particularly given the standardised nature of these assessments.
- **Follow-ups on TIAs to controllers via the data exporter**: Requiring these adds administrative layers without clear additional protection.
- **Notification of any changes to BCRs**: Only significant changes should trigger mandatory notification. Minor updates, such as the addition or removal of group legal entities, do not materially affect processing, so notifying controllers would create disproportionate administrative burden.
- **Notification of changes affecting processing conditions in time for controllers to object or terminate**: Including sub-processor changes under this requirement is redundant, as such notifications are already covered under existing Data Processing Agreements.

In general, accountability programs, such as BCR, should focus on the outcomes that organisations need to achieve. This approach allows organisations to implement rules, controls, and tools in ways that are effective for their unique culture, operations and proportional to the risks associated with their data processing activities. As long as organisations deliver the desired outcomes in terms of key elements of accountability and BCR, it is unrealistic for Supervisory Authorities to prescribe the exact methods by which these goals must be accomplished. Instead, Supervisory Authorities should emphasise the achievement of compliance and accountability, rather than mandating specific operational approaches.

5. Undermining the lead supervisory authority model

The approach suggested in the draft Recommendations risks subjecting organisations to oversight by multiple supervisory authorities in each jurisdiction to which data is transferred. This undermines the purpose of the lead supervisory authority model, increases fragmentation and legal uncertainty, and places additional strain on both organisations and supervisory authorities without improving compliance outcomes.

6. Strategic and global implications

BCR are recognised in multiple jurisdictions beyond the EU, including the UK, Dubai International Financial Centre, Brazil, Thailand and South Africa. Recent moves by additional countries to recognise BCR-Ps underscore their growing global relevance. The approach outlined in the draft Recommendations risks weakening this momentum and reducing interoperability at a time when trusted global data flows are increasingly essential.

The implications are particularly acute in data-intensive and AI-driven environments, where additional administrative layers may significantly impede responsible innovation and the development of trusted agentic AI ecosystems.

A workable and proportionate alternative

To address the concerns raised by Section 1.2, a practical and effective approach already exists. In all cases and in the reality of commercial relationships, there is always a contract between the EU controller and the initial processor entity, containing robust provisions on data protection, security, confidentiality, audit rights, and liability. This contract ensures compliance with Article 28 GDPR and provides strong legal leverage for the controller.

BCR-Ps should operate alongside these contracts to govern internal onward transfers within the processor's corporate group, providing consistent, enforceable protections and clear accountability across all entities involved. This layered model preserves flexibility, avoids unnecessary duplication, and maintains the commercial and regulatory incentive to use BCR-Ps, without imposing additional administrative burdens or prescriptive procedures that do not enhance individual protections.

Recommendations

In light of the above, CIPL respectfully invites the EDPB to:

- Reconsider or substantially clarify the language in Section 1.2 concerning the suitability of BCR-Ps for direct transfers from external controllers to BCR-P group members in third countries.
- Reaffirm BCR-Ps as a distinct, flexible, and accountability-driven transfer mechanism, rather than allowing them to converge toward the structure and rigidity of SCCs.
- Ensure a proportionate, outcomes-based approach that preserves the incentives for organisations to invest in higher standards of compliance and governance.
- Provide on-going leadership and focus on how to evolve and elevate BCR further, especially in relation to global trends in certification and third party accountability agents, and promote BCR adoption as an effective accountability program that delivers both local compliance with GDPR and enables data transfers.

CIPL would welcome the opportunity to engage further with the EDPB on these issues and to contribute constructively to the evolution of BCR as a scalable, future-proof accountability mechanism for international data transfers.

Sincerely,

Bojana Bellamy
President
Centre for Information Leadership