MORRISON | FOERSTER

GUSTAV MAHLERPLEIN 28
AMSTERDAM, 1082 MA
THE NETHERLANDS

TELEPHONE: +31 20 299 1889

WWW.MOFO.COM

MORRISON & FOERSTER LLP

AMSTERDAM, AUSTIN, BERLIN, BOSTON, BRUSSELS, DENVER, HONG KONG, LONDON, LOS ANGELES, MIAMI, NEW YORK, PALO ALTO, SAN DIEGO, SAN FRANCISCO, SEATTLE, SHANGHAI, SINGAPORE, TOKYO, WASHINGTON, D.C.

March 1, 2026

Writer's Direct Contact
+32 23407369
AvanderWolk@mofo.com

GLOBAL PRIVACY ALLIANCE
COMMENTS ON THE DRAFT RECOMMENDATIONS ON PROCESSOR BINDING CORPORATE RULES
pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

A. Introduction

We are writing on behalf of the Global Privacy Alliance ("**GPA**") in response to the public consultation from the European Data Protection Board ("**EDPB**") on the recommendation ("**the Recommendation**") governing Binding Corporate Rules for Processors ("**BCR-P**").[1] We welcome the opportunity to provide comments on this initiative and to contribute to the ongoing development of practical, effective, and legally robust mechanisms for international transfers of personal data under EU data protection law.

The GPA is a coalition comprised of a cross section of global businesses from the financial services, consumer products, cloud computing, computer software, communications, electronic commerce, health, pharmaceutical, professional services, and travel/tourism sectors. GPA members regularly engage in complex, multinational data processing activities and rely on a variety of transfer mechanisms to support global operations, service delivery, and innovation. The GPA works to encourage responsible global privacy practices that enhance consumer trust while preserving the free flow of information that underpins modern international commerce.

Members of the GPA take their privacy and data protection obligations very seriously and have substantial practical experience with the design, implementation, and operation of Binding Corporate Rules, including BCR-Ps. While the GPA supports efforts to improve clarity, consistency, and transparency in the application of BCR-Ps, it is concerned that certain aspects of the revised framework risk increasing administrative burden and reducing the effectiveness of BCR-Ps as a scalable and meaningful transfer solution. In particular, the exclusion of direct transfers from external controllers to processor group entities located outside the EEA represents a material change with significant practical implications for global service delivery models. This proposed shift would also create divergence from the approach currently accepted

[1] EDPB, 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), Adopted for public consultation 15 January 2026.

by the UK Information Commissioner's Office, placing organizations that maintain both EU and UK BCR-Ps in a fragmented and operationally challenging position.

The views expressed in this submission generally reflect the views of GPA members. While all members support the overall approach set out herein, certain points may be more relevant to some members than others. This submission is provided for consultation purposes only and does not represent the views of any individual member of the organization.

B. Key Criticisms and concerns

a) **Description of the issue**

The Recommendation introduces, in Section 1.2, a clarification regarding the scope of BCR-Ps that constitutes a notable development compared to prior iterations of the referential. The Recommendation provides 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 processors members of the BCR-P Group in third countries. For such a transfer, a different transfer tool under Article 46 is required instead*"[2].

Under this approach, where an external controller (typically a customer) established in the EEA (or otherwise subject to the GDPR) wishes to transfer personal data directly to a non-EEA processor entity that is part of a group with approved BCR-Ps, the controller would be required to rely on an alternative transfer mechanism under Article 46 GDPR. In practice, this would typically involve the use of the Standard Contractual Clauses ("**SCCs**") adopted by the European Commission pursuant to Article 46(2)(c) GDPR, or another appropriate safeguard such as an approved code of conduct or certification mechanism, where available.

By contrast, the Recommendation frames BCR-Ps as applicable only in scenarios where personal data are first transferred by the customer controller to a processor group entity established in the EEA, and are then transferred onward within the same group to a sub-processor entity located in a third country.[3] In other words, BCR-Ps would operate solely as a mechanism governing intra-group onward transfers, rather than as a comprehensive safeguard capable of covering the initial controller-to-processor transfer to a non-EEA group entity. This is not only a clear departure from the original intent of the BCR-Ps and prior guidelines, but it also creates an unnecessary practical burden that provides for no additional protection to personal data transferred.

[2] Recommendation, p. 5.
[3] Recommendation, p. 5.

b) Inconsistency with the original rationale of BCR-Ps and prior guidelines

BCR-Ps were developed to address the realities of global outsourcing and cross-border service delivery. They recognize that multinational processor groups operate integrated infrastructures, with processing distributed across multiple jurisdictions. The purpose of BCR-Ps is to provide a single, coherent framework that governs those internal transfers in a consistent and enforceable manner.

Their core value lies in ensuring that, once personal data enter the processor group, they are subject to uniform standards, binding commitments, audit controls, and enforceable rights, irrespective of the specific entity or country where the processing takes place. The level of protection should not depend on internal routing choices but on the group-wide obligations approved by supervisory authorities. Given the existence of SaaS cloud based systems, putting in a requirement that data flow in a particular order rather than being protected irrespective of the data flow is an outmoded concept.

This purpose of the BCR-P was not only recognized by the Article 29 Working Party (WP29) but explicitly provided for when it first (and later updated) the framework for approval of BCR-Ps. In its Working Document setting up the framework for the structure of Binding Corporate Rules for processors, originally dating from 2012, and then updated in 2018 when GDPR came into force, the WP29 explicitly provided that BCR-Ps can be used as a transfer tool designed to provide appropriate safeguards for transfers of personal data from controllers to processors within the same group, including where the receiving processor entity is located in a third country irrespective of the order and specific data flow. As expressly stated:

> "*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****; whereas BCRs for Controllers (BCR-C) are suitable for framing transfers of personal data from controllers established in the EU to other controllers or to processors established outside the EU within the same group.* ***Hence the obligations set out in the BCR-P apply in relation to third party personal data that are processed by a member of the group as a processor according to the instructions from a non-group controller***."[4] [emphasis added]

There can be no doubt about the interpretation of this wording, and the market has accordingly relied upon this guidance. The currently contemplated approach represents a significant – and as we will explain below: unnecessary – shift from the way BCR-Ps have historically been

[4] Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (WP 257 rev.01), last revised and adopted on 6 February 2018, p. 2.

designed and intended, and as a result thereof, implemented in practice. Excluding controller-to-processor transfers solely because the first recipient is outside the EEA ignores the very safeguards that BCR-P are meant to provide and elevates formal location over substantive protection.

Excluding certain transfers solely because the first receiving group entity is located outside the EEA shifts the focus from substantive safeguards to the formal sequencing of transfers. The risk profile of the processing does not change based on that initial entry point.

c) Why this change is problematic in practice

Beyond conceptual inconsistency, the revised approach creates significant operational challenges.

Global processor groups typically operate on a function-based delivery model. Processing activities are carried out where the relevant expertise, infrastructure, or service teams are located. In many cases, this is outside the EEA.

Within these structures, EEA-based group entities often perform a contractual, coordination, or client-facing role. They conclude the processing agreement with the controller and oversee service delivery. However, they may not carry out the substantive processing activities themselves. Those activities are frequently performed directly by group entities established in third countries.

Processor BCRs were developed precisely for such global service models. They were intended to reflect operational reality and to provide a single, internally binding framework governing processing across the group. The BCR-P framework was designed in the context of multinational processor groups operating across multiple jurisdictions and delivering services through integrated group structures. Supervisory authorities are therefore very well aware of how these delivery models function in practice. This is particularly so as data ecosystems and data flows are becoming increasingly complex, including in cloud-based and agentic AI environments where processing chains are dynamic and non-linear. A rigid sequencing requirement based on the location of the first recipient does not reflect this technical reality and risks rendering BCR-Ps unfit for the future.

The revised approach would require organizations to adjust their structures for formal compliance reasons only. In practice, they would face two options.

First, they could restructure their data flows so that personal data are artificially routed via an EEA group entity before being accessed by a non-EEA processor entity. At best, such restructuring would merely alter the formal transfer sequence without changing the level of protection afforded to the data. At worst, by introducing intermediary entities, it may ultimately increase the volume and frequency of transfers, thereby potentially increasing security risks and weakening protection.

Second, organizations could maintain parallel transfer mechanisms. In that scenario, SCCs would be used for direct transfers from an EEA controller to a non-EEA processor entity, while BCR-Ps would apply only to intra-group onward transfers. This would only increase contractual complexity, documentation, and compliance costs.

Importantly, this shift does not result in a higher level of protection. Approved BCR-Ps are already recognized as providing appropriate safeguards under Article 46 GDPR. They are subject to supervisory authority approval, binding effect across the group, audit requirements, and enforceable rights for both data subjects and controllers.

Notably, certain structural elements of BCR-Ps provide safeguards that go beyond what is embedded in the SCCs. In particular, BCR-Ps require the designation of at least one liable BCR Member established in the EEA that accepts responsibility for breaches committed by non-EEA group members and certain external sub-processors, including the obligation to remedy violations and pay compensation.[5] While the SCCs provide for liability and joint and several responsibility (Clause 12), they do not require the prior designation of a single EU-based entity that centrally assumes group-wide liability as a structural feature of the transfer mechanism.

In addition, BCR-Ps incorporate a shift in the burden of proof: where a data subject or controller can demonstrate damage and facts making a breach *likely*, it is for the liable BCR Member to prove that no breach occurred or that the non-EEA entity was not responsible.[6] The SCCs do not contain an equivalent mechanism.

Furthermore, BCR-Ps impose ongoing governance and transparency obligations at group level, including the requirement to keep the BCR framework updated and to maintain and provide to the Lead Supervisory Authority an up-to-date list of the entities bound by the BCR-Ps, on an annual basis.[7] Thus, replacing or supplementing BCR-Ps with SCCs does not, in itself, strengthen substantive protection. It primarily introduces additional paperwork.

[5] Recommendation, Section 1.4.
[6] Recommendation, Section 1.6.
[7] Recommendation, Section 11.

There is also a practical risk. Under a BCR-P framework, processor groups typically conduct regular internal reviews, audits, and updates to ensure continued compliance. If direct controller-to-processor transfers move outside the BCR-P perimeter and are addressed only through SCCs, there is a risk that the integrated governance model supported by BCR-Ps becomes fragmented. This may ultimately weaken, rather than enhance, the overall coherence of transfer compliance.

As such, the approach of the Recommendation suggests that SCCs are more effective and better than BCR-Ps for certain transfer scenarios, without a clear demonstrable increase in protection. If BCR-Ps are intended to represent a robust and high-standard transfer mechanism, it is unclear what regulatory objective is achieved by excluding direct controller-to-processor transfers from their scope.

d) **Impact on controllers and processors**

These structural changes have direct consequences for both controllers and processors groups.

Controllers reasonably expect BCR-Ps to provide a comprehensive and stable framework for international transfers within a processor group. Once approved, BCR-Ps are understood to offer legal certainty for global processing arrangements.

If direct controller-to-processor transfers to non-EEA group entities are excluded, controllers and processors will need to revisit existing arrangements. This will entail renegotiating contracts, implementing SCCs, and updating transfer assessments to address transfers that companies previously legitimately considered covered. Since BCR-Ps were first made possible in 2012, WP29 guidelines have consistently and explicitly recognized BCR-Ps being able to address the initial controller-to-processor transfers. It can come as no surprise that the market for over 14 years has relied on this interpretation. The contemplated change in approach will bring about a tremendous administrative burden to reassess and restructure such transfers.

For processor groups, the exclusion materially reduces the operational and, frankly, commercial value of BCR-Ps. Significant resources are required to design, obtain approval for, and maintain BCR-Ps. If they no longer cover a core category of transfers in global service delivery, the business case for relying on BCR-Ps – over intracompany SCCs for example, becomes weaker, if not effectively non-existent. This raises legitimate questions as to the practical benefit achieved by the change.

Conclusion

In conclusion, we urge the EDPB to not further pursue the contemplated change in approach regarding the suitability for BCR-P to legitimize EEA-controller to non-EEA processor transfers.

We very much appreciate the opportunity to provide these comments and would be happy to answer any questions that may arise.

With kind regards,

Alex van der Wolk