noyb’s comments on the Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Article 47 GDPR)

noyb welcomes the invitation of the EDPB to provide comments on the draft Recommendations 1/2022 (“the Recommendations”). Please find in this document our comments on the Recommendations for the consideration of the members of the EDPB.

The Recommendations are meant to provide a consolidated standard application form for the approval of Binding Corporate Rules (‘BCRs”) for controllers. They also clarify the elements to be found in BCRs, besides providing explanations and comments on the different BCRs requirements. The Recommendations repeal previous Article 29 Working Party documents WP256 and WP264, while also building upon these documents, the CJEU “Schrems II decision” (“Schrems II”), and the Standard Contractual Clauses (“SCCs”) adopted by the EU Commission on 4 June 2021. BCRs are explicitly mentioned – together with SCCs – as means to provide for appropriate safeguards under Article 46(2) GDPR. Both instruments can be used to transfer data outside of the EU in the absence of an adequacy decision.

Section I exposes the context in which SCCs can be used and the impact the decision of the CJEU in Schrems II on the transfers relying on the SCCs.

Section II explains why noyb considers that the role of the supervisory authorities and of the EDPB is too limited in scope when it comes to the review of the transfers covered by the BCRs as approved under the mechanisms provided for by the GDPR.

I. SCCs as appropriate safeguards under Article 46 GDPR

The following elements should be noted regarding the use of SCCs:

SCCs are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors not established in the EU and, consequently, independently of the level of protection guaranteed in these third countries.
In so far as those SCCs cannot provide guarantees beyond contractual obligations to ensure compliance with the level of protection required under EU law, the CJEU confirmed that **supplementary measures** must be adopted to meet that level of protection.¹

Following the *Schrems II* decision, the EDPB adopted its Recommendation 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. These Recommendations were adopted to provide guidance to data exporters “with the complex task of assessing third countries and identifying appropriate supplementary measures where needed.”²

As the Advocate General stated in his opinion in the *Schrems II* case, “the contractual mechanism set out in Article 46(2)(c) of the GDPR is based on responsibility being placed on the exporter and, in the alternative, the supervisory authorities. It is on a case-by-case basis, for each specific transfer, that the controller or, failing that, the supervisory authority will examine whether the law of the third country of destination constitutes an obstacle to the implementation of the standard clauses and, therefore, to an adequate protection of the transferred data, so that the transfers must be prohibited or suspended.”³

A data exporter using SCCs to transfer data outside of the EU must, **prior to any transfer**, ensure that nothing in the laws and practices of the third country of destination prevents the data importer to meet its obligations under the SCCs.⁴

Under the SCCs⁵, as revised after the *Schrems II* decision, the data exporter and the data importer contractually **warrant** that the data importer can meet its obligations under the SCCs.⁶ In this regard, both parties should conduct an **assessment of the protection of data in the relevant third country** under Article 14 (b) of the SCCs.

Under Clause 14 of the SCCs⁷, the data exporter shall identify appropriate measures when it considers that the data importer can **no longer fulfill** its obligations under the SCCs. The data exporter shall suspend the transfer if it considers that no appropriate safeguards for such transfer can be ensured or if instructed by the competent supervisory authority.

The SCCs do not provide for a mandatory notification mechanism to the supervisory authority. Consequently, **supervisory authorities do not review the supplementary measures before the beginning of the transfer** covered by the SCCs. Authorities would then only intervene when they are informed that an appropriate level of protection of the data cannot be provided in the third country of destination. However, authorities can be informed by the data exporter to receive instructions under Article 14 of the SCCs, or via a complaint filed by a data subject.

---

¹ CJEU, C-311/18, *Schrems II*, §133.
² See EDPB Recommendation 1/2020, Executive Summary.
³ Opinion of the Advocate General, 19 December 2019, C-311-18, §126.
⁴ See CJEU, C-311/18, *Schrems II*, § 142.
⁵ Commission Implementing Decision of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679.
⁶ See Clause 14(a) of the SCCs.
⁷ Clause 14 (e) and (f) of the SCCs.
II. The role of the supervisory authorities in the approval of BCRs

The present section explains why noyb thinks that the role of the supervisory authorities should be different in the case of BCRs. Before developing the reasons behind this conclusion, the paragraph below explains the differences between BCRs and SCCs.

a) The use of BCRs for transfers outside of the EU/EEA

While BCRs were introduced by the Article 29 Working Party without formal existence under the former Directive 95/46, BCRs were explicitly recognized as appropriate safeguards by the GDPR.

Contrary to SCCs, BCRs need to be approved by a supervisory authority, after an Opinion of the EDPB as per Article 64(1)(f) GDPR, and before the transfer begins. Several BCRs have already been subject to an Opinion of the EDPB before being approved by the competent supervisory authority.\(^8\)

For these reasons, the adoption of a set of BCRs is usually seen as a source of legal certainty for organisations relying on them to perform transfers within the organisation. Once approved by the competent supervisory authority, the transfer could indeed be deemed compliant with the GDPR and the companies could rely on the BCRs to conduct the transfer if they complied with the set of rules contained herein.

b) The role of the supervisory authorities in the approval of BCRs

We note that the Recommendations, subject to public consultation, limit the assessment of the BCRs to certain requirement of the GDPR. The Recommendations consider that it is “the responsibility of each data exporter to assess, for each transfer, on a case-by-case basis, whether there is a need to implement supplementary measures in order to provide for a level of protection essentially equivalent to the one provided by the GDPR.”\(^9\)

In its previous Recommendations 1/2020, the EDPB already reached the same conclusion that the reasoning in the Schrems II decision would also apply to other transfer mechanisms like BCRs.\(^10\) The same wording has also been used in the Opinions of the EDPB and the decisions of supervisory authorities approving the BCR after the Schrems II decision.\(^11\)

According to the EDPB, “the Court highlighted that it is the responsibility of the data exporter and the data importer to assess whether the level of protection required by EU law is respected in the third country concerned in order to determine if the guarantees provided by the SCCs or the BCRs can be complied with in practice”.\(^12\)

---

\(^8\) See for example: EDPB Opinion 29/2022; EDPB Opinion 07/2022; EDPB Opinion 26/2022; EDPB Opinion 21/2022; EDPB Opinion 23/2022.

\(^9\) See Recommendation, § 10.

\(^10\) See EDPB Recommendation 01/2020, §62.

\(^11\) See for example: EDPB Opinion 29/2022, p. 4; EDPB Opinion 07/2022, p. 5; EDPB Opinion 26/2022, p. 4; EDPB Opinion 20/2022, p. 4; EDPB Opinion 23/2022, p. 4.

\(^12\) See EDPB Recommendation 01/2020, §65.
We also observed that the Recommendations include a text in the section “Elements to be found in the BCR-C” that is almost identical to the text of the SCCs when it comes to the obligations regarding the law and practice in the third-country. According to the EDPB, organisations relying on BCRs would therefore be subject to obligations coming from the SCCs adopted by the European Commission.

c) noyb’s position on the role of supervisory authorities

noyb does not support the view that the reasoning of the CJEU in Schrems II should be applied to the BCRs framework, putting the exclusive responsibility on the data exporters to assess the level of protection in a third-country. On the contrary, we think that the approval of a set of BCRs should also cover the assessment of the level of protection in the third country, the necessity to adopt supplementary measures, and the validation thereof.

First, the CJEU never confirmed that the responsibility of the compliance with third-country legislation would be the responsibility of the data exporter in the case of BCRs. The Opinion of the Advocate General, to which the Court refers in Schrems II, only reached this conclusion when it comes to the SCCs.\(^{13}\)

Moreover, as explained under Section I, since they are not notified of the existence of the transfer when SCCs are used, supervisory authorities are not in a position to make a prior assessment of the legislation of third countries and of the potential supplementary measures. However, the same is not true when it comes to BCR since:

- BCRs need to be notified to the competent supervisory authority and approved before the transfer can start;
- organisations applying for BCRs share all relevant elements on the transfers covered with the supervisory authorities which are therefore in a position to perform a full assessment of the transfer at stake.\(^{14}\)

Furthermore, EDPB members are invited to conduct an assessment of the level of protection in the third country and to make it available to the supervisory authority upon request.\(^{15}\) It remains unclear why the BCRs application only contains a commitment to have conducted such assessment. The BCRs table explicitly refers to the right of the supervisory authority to request the assessment. This assessment should therefore be communicated to the supervisory authority at the moment of the application by the organisation filing a BCRs form.

Besides, the Recommendations contain the following statements:

“The approval confirms that the requirements set out in Article 47 GDPR are met, and therefore, that the commitments included in the BCR will provide for appropriate safeguards in the sense of Article 46 GDPR”\(^{16}\)

\(^{13}\) Opinion of the Advocate General, 19 December 2019, C-311-18, §126.
\(^{14}\) Like the categories of data involved, the countries of the different companies of the group, the security measures adopted, or the legal basis for the processing.
\(^{15}\) See 5.4.1. of the table of “elements to be found in the BCR”.
\(^{16}\) See Recommendations, §9.
“the responsibility of each data exporter to assess, for each transfer, on a case-by-case basis, whether there is a need to implement supplementary measures in order to provide for a level of protection essentially equivalent to the one provided by the GDPR.”

“supplementary measures are in the responsibility of the data exporter, and as such, are not assessed by supervisory authorities (hereinafter “SAs”) as part of the process of approval of BCR.”

These statements seem contradictory and not in line with the role of supervisory authorities for the following reasons:

- The EDPB confirms that BCRs provide for appropriate safeguards, that the requirements of the GDPR are met, and that the transfer can take place. However, this first statement seems contradicted by the second statement which implies that the approved BCRs are not enough if supplementary measures need to be adopted.
- Supervisory authorities are vested with the power and the duty to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down in the GDPR. Therefore, the monitoring of transfers should not be an option for supervisory authorities but a duty when they are in a position to monitor such transfers, as it is the case for BCRs.

Organisations usually invest a lot of resources in the assessment of the level of protection in third countries. It would be ineffective to ask organisations relying on BCRs to conduct such assessments and ignore them at the same time.

If organisations can no longer fully rely on BCRs for all aspects of their transfers, it would deprive BCRs of their legal certainty, which made them popular and suitable transfer mechanism in the first place.

### III. Conclusion

Considering the above, noyb invites the EDPB to:

- depart from its original view, according to which the responsibility to assess the level of protection in third-countries would primarily lie on the controllers;
- provide that the future BCR applicants and existing BCR-C holders shall submit all relevant information to the competent supervisory authority regarding the level of protection in third countries and the supplementary measures envisaged when they consider that such measures are required to ensure a level of protection essentially equivalent;
- specify that the supervisory authorities shall review and approve the entire scope of the BCRs, including the level of protection in the third country and the supplementary measures suggested by the BCR holder to ensure an adequate level of protection of the data in the third countries identified in the BCR application.

---

17 See Recommendations, §10.
18 CJEU, C-311/18, Schrems II, § 107.