XpertDPO submission to the EDPB public consultation on 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)

Submission timeframe:

January 10, 2023

XpertDPO is an information governance service provider that offers data security, governance, risk and compliance, GDPR and ISO consultancy solutions to clients in Ireland and the UK. We are one of the leading providers of Outsourced Data Protection Officer Services in Europe. We also specialise in offering Nominated European Representative Services to non-EU based organisations.

XpertDPO welcomes the European Data Protection Board's 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) and the opportunity to provide written comments on the proposed recommendations.

The updated guidance is particularly welcome in light of the Court of Justice of the European Union's Schrems II ruling and provides clarity for companies relying on Binding Corporate Rules for international data transfers. We would, however, like to make some suggestions to contribute to the public consultation that we believe the EDPB should take into consideration.

Below are our contributions:

Section 1 Introduction

Among the stated goals of these EDPB recommendations is to provide additional guidance and to ensure a level playing field for all BCR applicants. In line with this, XpertDPO suggests the EDPB provide further clarity on the timeframes for the BCR-C approval process and on the level of regulatory involvement throughout the process.

For example, standardised timeframes for the lead supervisory authority to issue a draft approval decision, for the EDPB to issue its opinion on that decision, and for the finalised decision to be issued to the applicant could be added to the introduction section, point 9 (p5). Such clear standardised guidance is in line with the goal of the GDPR to harmonise data protection laws and practices across all the member countries, and as a provider of consultancy services it would be useful to be able to provide this information to clients considering BCR-Cs as a mechanism for international data transfers.

Point 13 (p5) states that *"the EDPB expects all BCR-C holders to bring their BCR-C in line with the requirements set out below. This includes BCR-C that have been approved before the publication of these Recommendations."* Again, it would be helpful if the EDPB could clarify if it has a timeframe in mind for this to be completed, and what level of consultation is required with the lead supervisory authority during this process.

Section 3 Elements and Principles to be found in BCR-C

2.1 Description of the material scope of the BCR-C includes a footnote (footnote number 18, p25) that states *"information on the transfers must be exhaustive in that every transfer or set of transfers must be described. This does not mean that the information must be provided with a high degree of specificity or granularity. Where the description provided by*

the applicant is too broad, general or vague, the applicant should be able to explain why it is not in a position to provide more detailed information."
This footnote is a new addition and, in our opinion, only adds confusion, as the language is somewhat contradictory. The clause itself provides clear information about what is requested: *"The BCR-C must, in particular, specify per transfer or set of transfers (for example, by means of a table):*

- *the categories of personal data;*
- *the type of processing and their purposes;*
- *the categories of data subjects (e.g. data related to employees, customers, suppliers and other third parties as part of the Group's respective regular business activities); and*
- *the third country or countries."*

If the EDPB is of the view this clause requires further clarification it should be mindful of the language used to avoid any confusion. For example, it may be enough to state 'Every transfer or set of transfers must be described in the BCR-C,' if this is the point intended to be emphasised.

3.1 Suitable training programme (p26-27) specifies that this information must be detailed on the BCR-C but not on the application form, as was previously the case in the WP256 guidelines. However, **Section 6 Effectiveness** (p14) of the application form requires information on training and awareness raising for employees to be completed. It would be helpful if the EDPB could clarify if information on training programmes should be included in both the BCR-C and the application form.

5.1.3 Security & Personal data breach notifications (p35) states *" The BCR-C should include a commitment to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk(s) for the rights and freedoms of natural persons (see Article 5(f) and Article 32 GDPR). It is not mandatory to copy-paste the wording of such GDPR provisions. However, the BCR-C need to create those obligations in a sufficiently elaborated manner that is in line with the content of these provisions."* XpertDPO suggests that this be reworded to specify that the BCR-C should detail the measures used to ensure security of data, in line with the requirements as set out by Article 47 (2)(d) of the GDPR.

<u>General query</u>

In circumstances where an adequacy decision is subject to a sunset clause, as is currently the case with the UK, should this fact be noted on a BCR and does a process need to be in place to review the specifics of transfers should the adequacy decision not be renewed? Guidance from the EDPB on this would be much appreciated.

If you would like to discuss any of these comments or require additional information, please contact us at info@xpertdpo.com