BINDING CORPORATE RULES

BENEFITS, APPROVAL PROCESS AND DOCUMENTATION

1. INTRODUCTION

Binding Corporate Rules ("**BCR**") are recognised by Article 46 (2)(b) of the General Data Protection Regulation 2016/679 (the "**GDPR**") as a mechanism to legitimise intra-group international transfers of personal data originating from the EU.

In essence, a set of BCR is a global code of practice based on European privacy standards, which multinational organisations draw up and follow voluntarily, and national data protection authorities approve in accordance with the GDPR. Once the BCR of a corporate group is approved, all of the entities covered by the BCR can transfer personal data within the group without any further contractual arrangements (such as the Standard Contractual Clauses) needing to be in place.

2. BENEFITS OF BCR

Before embarking on a BCR project, organisations must realistically assess whether their own internal culture is aligned with the BCR approach. The BCR concept is ideally suited to those organisations that wish to apply a consistent and effective approach to privacy compliance throughout the world.

In addition to acting as a mechanism to legitimise data transfers, BCR should be seen as a framework for a global privacy compliance programme, which has the following benefits:

- Establishing a consistent way of rolling out and publicising privacy practices across the organisation.
- Assisting organisations with meeting their accountability obligations under the GDPR.
- Providing legal certainty regarding the ability to carry out global data exports.
- Contributing to the efficient management and exploitation of a key business asset.
- Turning complex data protection obligations into user-friendly guidelines for data handlers and employees.
- Reducing regulatory scrutiny.

Ultimately, adopting and implementing BCR should not be an administrative burden, but a natural way of managing personal data for those organisations that look at privacy and data protection as critical aspects of their operations.

There is a clear overlap between the obligations on an organisation under GDPR, and those required under a BCR, the main difference being that the BCR standards will apply not only to the corporate entities within the EU, but to all entities to which personal data may be transferred from the EU. The work that a corporate group has undertaken in preparation for GDPR will be of great value in relation to a BCR application.

3. BCR APPROVAL PROCESS

The BCR approval process is set out in Article 47 of the GDPR with further detail provided by the Article 29 Working Party (now the European Data Protection Board) ("**EDPB**") in WP263.

In order to obtain BCR approval candidates must submit an application to the national data protection authority they consider to be the most suitable to lead the approval process based on criteria set out in WP 263. These criteria include:

(a) The location(s) of the group's European headquarters.

(b) The location of the company within the corporate group with delegated data protection responsibilities.

(c) The location of the company which is best placed (in terms of management function, administrative burden, etc.) to deal with the application and to enforce the BCR in the corporate group

(d) The place where most decisions in terms of the purposes and the means of the processing (i.e. transfer) are taken.

(e) The member state within the EU from which most or all transfers outside the EEA will take place.

If the chosen supervisory authority agrees to act as lead authority, it will confirm the position to the other supervisory authorities from which a corporate group will be seeking approval. The other supervisory authorities have an opportunity to object to the appointment which is why it is important to be able to make out as strong a case as possible why the chosen lead supervisory authority has been selected.

Once a supervisory authority has agreed to act as lead authority, and the other supervisory authorities to whom the application relates have not objected to the appointment, the **lead authority** reviews the BCR application and makes comments and suggested amendments. Once the lead authority is comfortable that the documents meet the BCR standards described below, it will circulate the BCR documents to **one or two other supervisory authorities** for a further review. These further supervisory authorities are able to make comments and propose amendments.

Once the lead authority and the further supervisory authorities are comfortable that the documents comply with the BCR requirements, the lead authority will circulate the BCR to the **remaining EU supervisory authorities** in jurisdictions where affected data subjects are located. The other concerned supervisory authorities may make comments within 1 month of receiving the draft BCR. After this period has expired, and the lead authority is satisfied that all comments have been addressed, the lead authority will provide the BCR and a draft decision to the EDPB.

The EDPB will then circulate the BCR to all supervisory authorities along with a draft opinion on the BCR. The other supervisory authorities will have eight weeks to make any suggested amendments (which may be extended by a further six weeks if the matter is particularly complex). If more than 50% of the supervisory authorities either (a) approve the BCR, or (b) do not make any objections to the BCR within the eight week period, the BCR will be deemed to be approved. If the agreed EDPB Opinion requires changes to the BCR, these will be communicated to the applicant by the lead authority. **The entire approval process from submission of the application form to approval by the EDPB is likely to take around 9 months to just over a year.**

4. CONTROLLER / PROCESSOR BCR

There are two separate types of BCR for controllers and processors: BCR-Controllers ("**BCR-C**") and BCR-Processors ("**BCR-P**").

BCR-C apply to transfers of personal data from controllers established in the EU or otherwise subject to the GDPR to other controllers or processors (established outside the EU) within the same group. An organisation typically processes personal data about its employees, customers, sponsors, suppliers and other business contacts as a controller. A corporate group should therefore adopt BCR-C to cover this type of personal data to legitimise international data transfers within the group.

BCR-P apply to transfers of personal data received from a controller established in the EU or otherwise subject to the GDPR which is not a member of the group which is then processed by the group members as processors and/or sub-processors.

5. DOCUMENTATION REQUIRED FOR BCR

5.1 Templates and checklists

In order to assist BCR candidates, the EDPB has issued:

- **Template application forms** (WP264 for BCR-C and WP265 for BCR-P) designed to focus applicants on the content of a BCR application and also to assist those data protection authorities reviewing applications to assess whether the required elements are contained within the application.
- **Tables setting out the consolidated approval criteria for BCR** (WP256 for BCR-C and WP257 for BCR-P). This clarifies the specific elements which must be contained in the BCR documentation and provides a set of criteria for approval.

5.2 Application Forms

There are two parts to both the BCR-C and BCR-P application forms.

Part I (Applicant Information) sets out the basis on which the lead authority has been chosen and includes information about:

- Structure and contact details of the applicant and of the group of companies.
- Short description of the data flows.
- Determination of the lead authority based on specified criteria.

Part II (Background Paper) of the application form sets out the details of how the group complies with the various approval criteria for BCR, including:

- Binding nature of the BCR.
- Effectiveness.
- Cooperation with supervisory authorities.
- Cooperation with data controllers (for BCR-P only).
- Description of processing and data flows.
- Mechanism for reporting and recording changes.
- Data protection safeguards.
- Accountability and other tools.
- Copy of the formal BCR.

5.3 **BCR policy document**

In addition to the information submitted in the application form, the BCR applicant is required to submit a copy of the formal BCR policy. This is a top level document, which sets out the rules that each member of the group will agree to comply with when it signs up to the BCR. The BCR Policy must be drafted with reference to Article 47 GDPR and also to the WP256 and WP257 Checklists and must include:

(a) Details of the types of transfers which will take place under the BCR, including details of data subjects, types of personal data and the countries to and from which personal data will be transferred.

(b) Commitments to comply with the data protection principles set out in the GDPR.

(c) The right for individuals to obtain redress if an entity acts in breach of the BCR.

(d) Details of how compliance with the BCR will be monitored internally.

(e) The procedure for handling and monitoring complaint handling and training.

(f) Mechanisms for cooperation with the supervisory authorities, for reporting legal requirements which may have a substantial adverse effect on the BCR and for updating the rules.

The BCR policy will be supported by **various procedures and policies**.

5.4 **Binding mechanism**

In addition, BCR applicants are required to have in place a mechanism which binds group members to comply with the BCR and to create third party beneficiary rights. This mechanism does not have to be in place at the date of the application. There are various types of binding mechanisms but the most universally recognised is an intra-group agreement.

6. OVERSEEING COMPLIANCE

In order to make the approval application and to ensure compliance with the BCR once it is approved, a corporate group is required to have, and demonstrate in the BCR application that it has, an **internal team which is responsible for administering and monitoring compliance** with the BCR.

We recommend establishing a central team with responsibility for and oversight of the BCR centrally, as well as appointing an employee with responsibility for compliance in each subsidiary or region, including outside the EU in the countries to which personal data will be transferred under the BCR. It is acceptable for the individuals in the BCR compliance team to overlap with those in the GDPR compliance team.

There is no requirement for the local appointees to be full time data protection or privacy specialists, but it is important to be able to demonstrate that there is a local point of contact in the countries where personal data will be transferred, to deal with queries on a local basis and to report to the central team.

The Data Protection Officer ("**DPO**") is expected to be an integral part of the internal BCR compliance team, and monitoring compliance with the BCR should be a significant part of the DPO role.