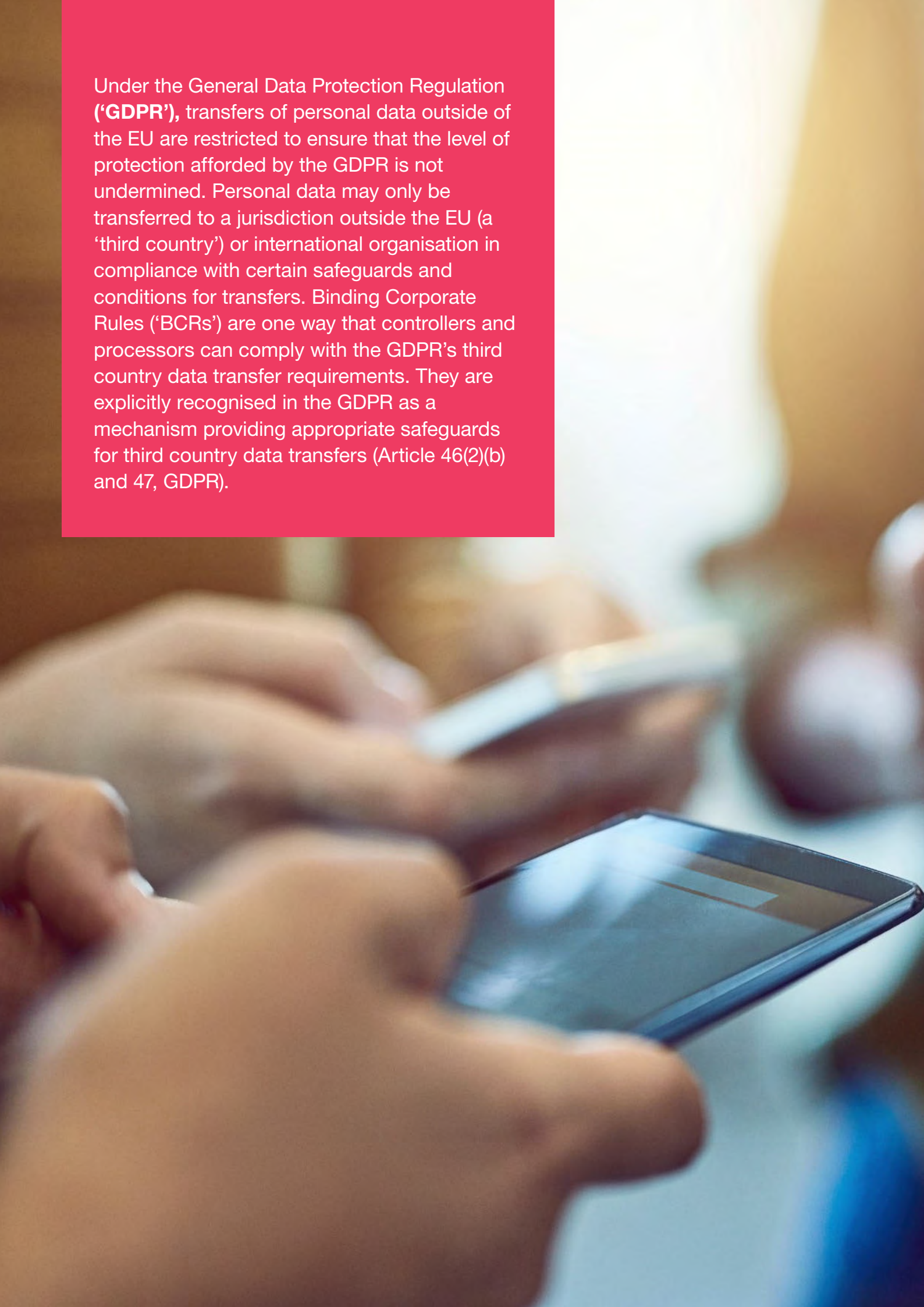
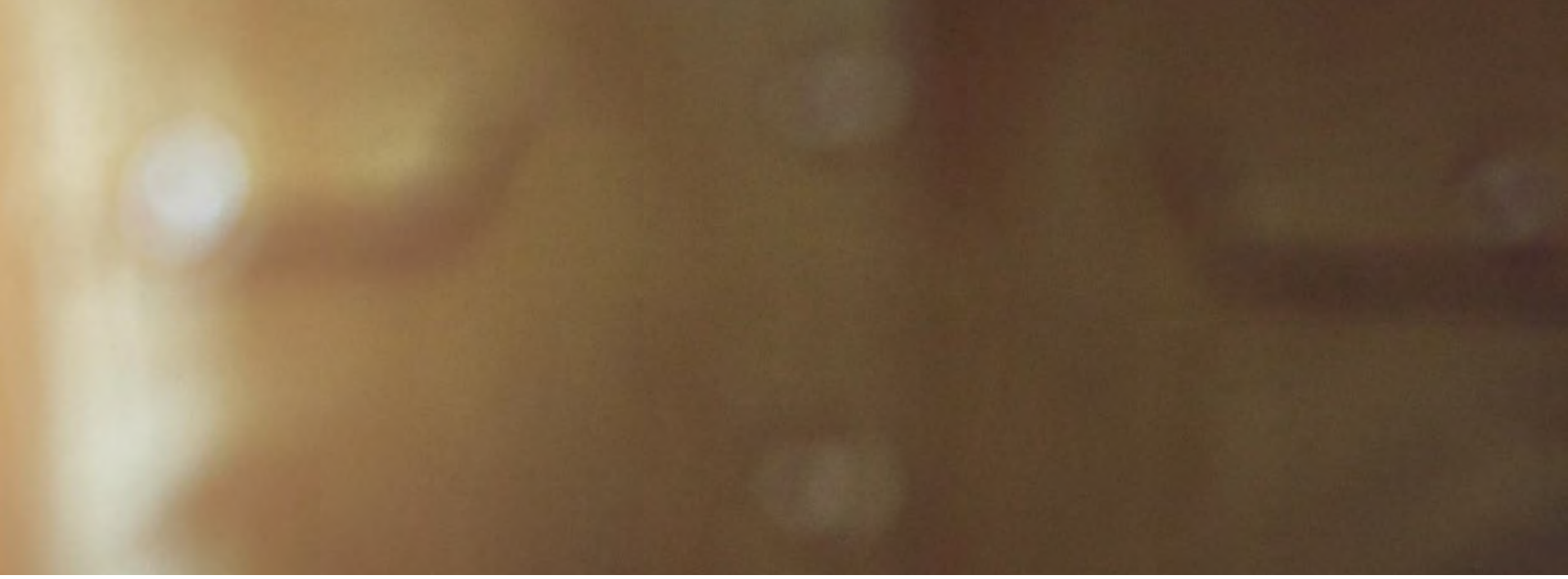
Binding Corporate Rules

The General Data Protection Regulation

pwc

Under the General Data Protection Regulation **('GDPR'),** transfers of personal data outside of the EU are restricted to ensure that the level of protection afforded by the GDPR is not undermined. Personal data may only be transferred to a jurisdiction outside the EU (a 'third country') or international organisation in compliance with certain safeguards and conditions for transfers. Binding Corporate Rules ('BCRs') are one way that controllers and processors can comply with the GDPR's third country data transfer requirements. They are explicitly recognised in the GDPR as a mechanism providing appropriate safeguards for third country data transfers (Article 46(2)(b) and 47, GDPR).





What are BCRs?

BCRs are legally binding and enforceable internal rules and policies for data transfers within multinational group companies and work in a way somewhat similar to an internal code of conduct. They allow multinational companies to transfer personal data internationally within the same corporate group to countries that do not provide an adequate level of protection for personal data as required under the GDPR.

BCRs ensure that all data transfers within a corporate group comply with the GDPR and must contain:

- data protection principles, such as transparency, data quality, and security;
- tools of effectiveness (such as audit, training and complaint handling); and
- an element proving that the BCRs are binding, both internally and externally.

There are two types of BCRs – Controller BCRs and Processor BCR's.

Controller BCRs

Controller BCRs are suitable for data transfers from controllers established in the EU to other group company controllers or to processors established outside the EU. They apply to entities within the same group acting as controllers and to entities acting as 'internal' processors.

Processor BCRs

Processor BCRs apply to personal data received from a controller established in the EU which is not a member of the group and then processed by group members as processors or sub-processors. These type of BCRs are an alternative to incorporating the EU Commission Standard Contractual Clauses ('SCCs') into service agreements with controllers.

This article will focus on Controller BCRs.

Why Binding Corporate Rules can be a better option than the Standard Contractual Clauses

BCRs can be tailored to fit the needs of the business and once implemented and operational, are much easier to maintain compared to intra-group contracts incorporating the SCCs. They also set a high standard for compliance with the GDPR which should reduce business exposure and are seen as the 'gold standard' for compliance. This can be very beneficial for brand image and reputation.

Additionally, BCRs provide a great degree of flexibility not found in other adequacy mechanisms, as the competent supervisory authority does not need to approve non-material updates to BCRs. This can save both time and costs.

Implementing BCRs also acts to further raise awareness of data protection compliance within a business and serves to demonstrate accountability, as required under the GDPR.

Whereas SCCs generally work well for smaller companies and bilateral data sharing, their use in a large multinational can be very cumbersome and impractical:

- SCCs may not be fit for purpose where there is a complex web of processing activities.
- Larger companies with many affiliates abroad often need to put in place hundreds of SCCs which can be very costly.
- Some EU member states require additional formalities, such as filing and approval of SCCs by the supervisory authority, making the process of implementing SCCs both lengthy and costly.

As well as the above, the future of the SCCs is currently uncertain with the **Schrems v Facebook** litigation currently before the Irish Supreme Court. This case concerns a challenge to the validity of the SCCs as a data transfer mechanism to the US with a possible referral to the CJEU to determine their legal validity.

[1] Article 29 Working Party Guidance (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf)

Application and approval process

The content of BCRs

BCRs should be tailored to the particular corporate group. WP29 Guidelines[1] provide a suggested framework for a set of BCRs to assist companies in drafting their own. The framework is not however a model set of BCRs and supervisory authorities will not accept a copy of this framework.

BCRs may consist of several documents so long as the legal relationship between such is clearly set out. One suggested approach is that the main principles for compliance will be set out in one document and that this will then be complemented by policies, guidelines, audit and training programs, etc.

There is a 'Standard Application Form for the Approval of Binding Corporate Rules' which can be found at the following URL: http://ec.europa.eu/newsroom/article29/document cfm?action=display&doc_id=51310

Main principles document

The main principles document will need to address the key principles provided for in the GDPR. This includes:

- transparency, fairness and lawfulness;
- data minimisation and accuracy;
- purpose limitation;
- storage period limitation; and
- security.

It should also provide guarantees regarding:

- processing of special categories of personal data;
- restrictions on transfers and onward transfers to external processors and controllers without BCRs;
- compliance with Article 28(3), GDPR for agreements with processors (both within the group and externally); and
- an obligation to notify data breaches to the EU BCR lead with the delegation of data protection responsibilities, the DPO, and the data subject (if applicable).

The scope of the personal data covered by the BCRs should also be set out.

Other elements

The following elements must also be addressed in the BCRs, either in the main principles document or associated documents:

- **Scope of application:** The BCRs must specify the data transfers to which they apply, the categories of personal data, the type of processing and its purpose, the types of data subjects, and identify any third countries where data is transferred.
- **Group structure:** The BCRs must specify the group structure, the list of entities bound by the BCRs and their contact details. It should also be stated whether they apply to all personal data transferred from the EU or to all processing of personal data within the group, whatever the origin.
- **Binding nature of BCRs[2]:** BCRs must be legally binding and governed by the law of an EU Member State (likely the law of the country of the EU BCR member). The BCRs must include a duty for each BCR member and its employees to respect the BCRs.
- **Accountability:** Every entity acting as a controller must be able to demonstrate compliance with the BCRs[3]. Processors should make information available to the controller to demonstrate their compliance with the BCRs, including through audits and inspections[4].

*Except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

[1] Article 29 Working Party Guidance (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp154_en.pdf)

[2] Article 27(2)(c), GDPR. WP 256 1.1, 1.2 https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798

[3] Article 4(2), GDPR.

[4] Article 28(3)(h), GDPR.

- **Complaint handling**[5]**:** There must be an established system that allows data subjects to complain about any BCR member. Any such complaints must be dealt with by a clearly identified department without undue delay, and in any event, within one month. Additionally, the people handling the complaints must have an appropriate level of independence in exercising their functions.
- **Third party beneficiary rights**[6]**:** The BCRs must grant data subjects the right to enforce BCRs as third- party beneficiaries.
- **Transparency:** Data subjects should be provided with the information in articles 13 and 14 GDPR and information on their third party beneficiary rights in relation to how their data is processed and how they can exercise those rights. Specifically, the BCRs must include clauses on liability and the data protection principles, and information must be provided in full or provide links to other data protection notices such as to privacy policies[7].
- **Easy Access**[8]**:** BCRs must contain the right for every data subject to have access to them. For example, relevant information should be published on the website or internet for employees.
- **Third country legislation**[9]**:** The BCRs must include a commitment that any third country legal requirements likely to have a substantial adverse effect on the guarantees of the BCRs will be reported to a competent supervisory authority; for example, any legally binding request for disclosure by law enforcement or state security authorities must be reported. The BCRs must also include a commitment that if there is a conflict between national laws and the BCRs, the EEA headquarter, the member with delegated data protection responsibilities, or any other relevant privacy officer or function, will take a reasonable decision on the appropriate action and consult with supervisory authorities if there is any doubt.
- **Right to lodge a complaint**[10]**:** Data subjects should be able to bring a claim before a supervisory authority in their home country, country of work, where the alleged infringement took place, before a competent EU court where the data exporter has an establishment, or in the data subject's country of residence.
- **Relationship with national laws**[11]: The BCRs should state that where local laws require a higher level of protection for personal data, the local laws will take precedence over the BCRs.
- **Cooperation with supervisory authorities**[12]: The BCRs must contain clear and unambiguous undertakings that all BCR members as a whole, and any members of the group separately, will cooperate with the relevant supervisory authorities, accept to be audited by the relevant supervisory authorities; and comply with the advice of relevant supervisory authorities.
- **Liability**[13]: The EEA member with delegated data protection responsibilities must accept responsibility for and agree to take the necessary action to remedy acts of other group members outside the EEA. The BCRs must also contain an obligation on the EEA member with delegated data protection responsibilities to pay compensation for damages arising from a breach of BCRs by any member of the group. There must also be a statement that the responsible EEA group member bears the burden of proof in relation to alleged breaches of BCRs by a group member outside the EEA.

---

[5] Article 47(2)(i), GDPR. WP29 256 1.4 https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798

[6] Article 28, 29, 79 GDPR. WP 256 1.3 https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798

[7] Article 47.2(g) GDPR.

Updates to BCRs

BCRs should include an obligation that significant changes to the BCRs or to the list of BCR members are notified to all group members and to the relevant supervisory authorities. Any significant changes to the BCRs must be communicated to data subjects. Certain modifications will also require a new authorisation from the relevant supervisory authorities.

It is possible to update BCRs without having to re-apply for authorisation, provided that:

- Personal data is not transferred to a new group member until the data exporter has ensured that the new member is effectively bound by the BCRs and can ensure compliance.
- An identified person or department keeps a fully updated list of members of the BCRs, keeps track of and records any updates to the BCRs and provides the necessary information to the data subjects or supervisory authorities on request.
- Any changes to the BCRs or to the list of BCR members should be reported once a year to the relevant supervisory authorities via the competent supervisory authority granting the authorisations, along with a brief explanation of the reasons justifying the update.

The BCRs should also contain an obligation that the group will ensure compliance with the above requirements for updates to the BCRs.

Binding nature

The above principles need to be binding within the corporate group, as against employees and subcontractors[14]. The documents likely to achieve this are:

- A resolution of the parent company's board to make the principles binding;
- An employee notice requiring application of the principles;
- Pro forma contract terms for use with subcontractors; and
- Intra-group contract that confers third party rights.

Further evidence

As well as the main principles document and the binding documents discussed above, the following also need to be documented:

- **Training**[15]
  Training on BCRs must be provided to those employees who have regular or permanent access to personal data. When seeking approval of BCRs, supervisory authorities will require evidence that the commitments in the BCRs are being respected. Such evidence may include examples and explanations of the training programme for employees regarding the BCRs; for example records may be kept about the training that employees receive such as records of the content of the training, attendee lists, and training schedules.
- **Audit programme**[16]
  The process for auditing compliance with BCRs on a regular basis will be documented and reported directly to the ultimate parent's board or to the DPO. The BCRs must also state that the audit programme will cover all aspects of the BCRs and ensure that any necessary corrective action will be taken.

  The data protection audit programme and plan must be clearly set out either in a document containing the group's data protection standards or in other internal procedure documents. The BCRs must also specify when the audits will take place (this must be on a regular basis).

  Additionally, audits must be carried out at the request of the DPO or at the request of any other competent function within the group, and the BCRs must state that the supervisory authorities can have access to the results of the audits on request.

  The BCRs must grant the supervisory authorities the right to carry out a data protection audit themselves (or independent auditors on their behalf), and each member of the group must accept that it could be audited by the supervisory authorities and abide by their advice on any issue related to the BCRs.

[14] WP29 256 1.1, 1.2
[15] WP29 256 2.1
[16] WP29 256 2.3

- **Compliance and supervision**[17] The BCRs must include a brief description of the internal structure, role, position and tasks of the DPO and the appropriate network created and must set out a system that guarantees awareness and implementation of BCRs within the corporate group.

Identifying a BCR lead[18]

Under the cooperation procedure, one supervisory authority acts as a BCR lead which liaises with the applicant and the other relevant concerned supervisory authorities to facilitate the approval of BCRs in all relevant jurisdictions.

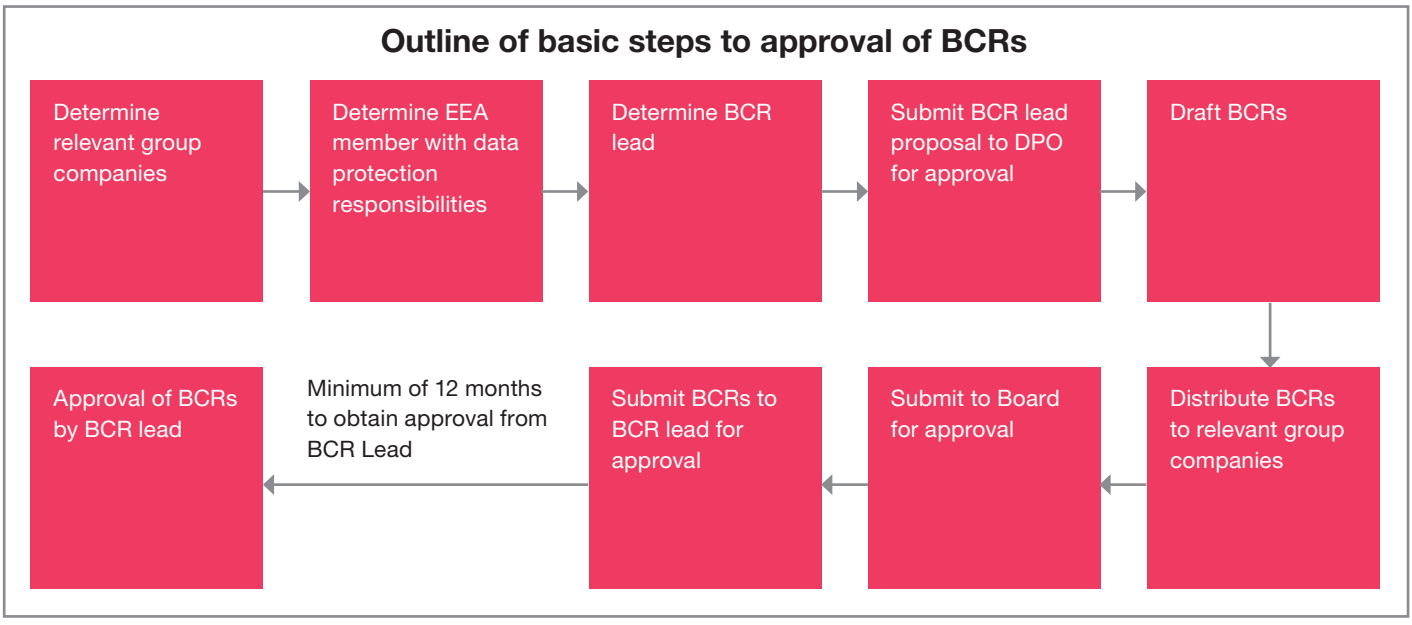
Before an applicant submits proposed BCRs (and the accompanying application form and documents), they need to identify a supervisory authority to act as the BCR lead for the purposes of the application. The applicant must justify why a particular supervisory authority should be the BCR lead.

When the ultimate parent or operational headquarters are located outside the EEA, the applicant should apply to the relevant supervisory authority based on the following criteria[19]:

- The location of the groups EEA headquarters.
- The location of the group company with delegated data protection responsibilities.
- The location of the company best placed to deal with the application and to enforce BCRs within the group.
- The location where most decisions in terms of the purposes and means of processing take place.
- The jurisdiction within the EEA from which most transfers outside the EEA will take place.

The Article 29 Working Party ('WP29') advises that particular attention will be given to the location of the group's EEA headquarters, and regardless of the applicants choice, the supervisory authorities have the discretion to decide among themselves which supervisory authority should be the BCR lead.

Outline of basic steps to approval of BCRs



[17] Article 47(2)(h) GDPR; WP29 256 2.4
[18] Article 60(1) GDPR, WP29 263.1
[19] WP29 263 1.2.

Cooperation procedure[20]

After the BCR lead has been determined, the BCR lead will begin discussions with the applicant and review the draft BCR documents. The BCR lead will then provide its comments on the proposed BCRs and a first revised draft will be produced. This draft will then be distributed to one or two supervisory authorities which will act as co-reviewers and help the BCR lead in their assessment. In normal circumstances the period for comments from co-reviewers will not exceed one month.

A consolidated draft is then created by the applicant and is sent to the BCR lead who will circulate it to all concerned supervisory authorities for comments. The period for comments on the consolidated draft will not exceed one month and silence is deemed to be agreement.

If there are any further comments then the BCR lead will send the draft back to the applicant and may resume discussions. Addressing each concerned supervisory authority's comments on the consolidated draft may be very time-consuming.

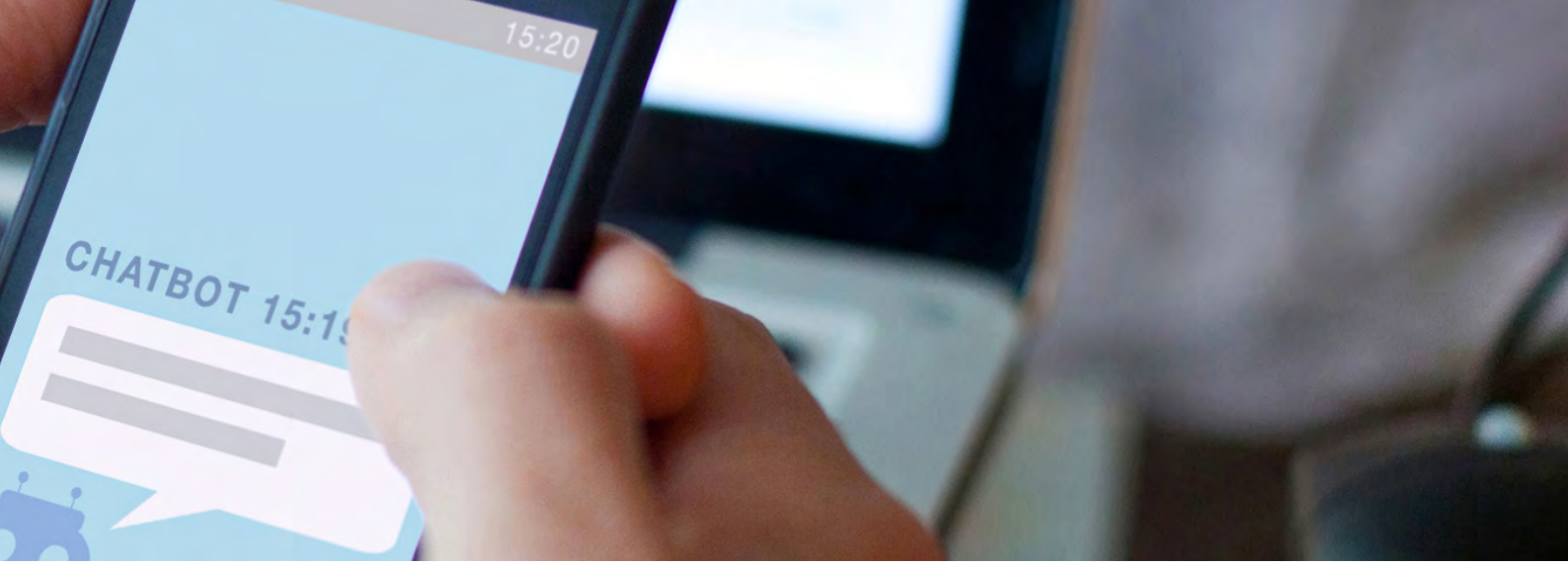
Approval process[21]

Once the BCR lead authority decides that the applicant has addressed the comments on the consolidated draft to a satisfactory standard, it will invite the applicant to send it the final draft. The BCR lead will then submit the draft decision to the European Data Protection Board (EDPB) on the 'final draft' of the BCRs along with the relevant documents and the views of the concerned supervisory authorities. If the EDPB opinion endorses the draft decision, the BCR lead will approve the draft BCRs and information and send all concerned supervisory authorities a copy of the BCRs.

Checklist of documents to be provided to supervisory authorities for the approval of BCRs

1. The main principles document
2. A document setting out third party rights (if third party rights clause is not contained in the main principles document)
3. Application form WP 264[22]
4. Documents to make the BCRs binding. (e.g. resolution of parent company board to make the principles binding; employee notice to require application of the principles; pro forma contract terms for use with subcontractors; intra-group contract which confers third party rights)
5. Supporting documents that demonstrate that commitments in the BCRs are being respected.

[20] WP29 263 2.
[21] WP29 263 2.
[22] Application form WP29 264



Examples of supporting documents to demonstrate commitment to BCRs

- Privacy Policies
- Employee guidelines for those who have access to personal data
- Data protection audit plan and programme
- Examples and explanation of training programmes for employees
- Documents demonstrating that the member of the group transferring data outside the EEA, and the EEA member with delegated data protection responsibilities has sufficient assets to pay any compensation resulting from breach of the BCRs
- A description of the internal complaint system
- A list of entities in the group bound by the BCRs
- A security policy for IT systems that process EU personal data
- A certification process to ensure that all new IT applications that process EU personal data are compliant with the BCRs
- Any standard contracts that are used with processors that process EU personal data
- A job description of the DPO or other persons that are in charge of data protection (e.g. Privacy Champions).

BCR Assurance

The effectiveness of a BCR may be assessed by submitting them to a formal audit and assurance assessment. As discussed above, BCRS contain a commitment to have their implementation audited/reviewed on a regular basis. Depending on the exact wording of the BCR, the organisation can commit itself to a certain level of review.

With the GDPR now in full operation and BCRs beginning to mature, PwC is now assisting clients in carrying out formal assurance and BCR audit engagements.

Contacts

Legal Services

Richard Chudzynski
Legal Data Protection and Privacy Leader

M: +971 56 417 6591
E: richard.chudzynski@pwc.com

Gordon Wade
Senior Data Protection and Privacy Lawyer

M: +971 50 143 5619
E: gordon.wade@pwc.com

Alice Gravenor
Data Protection and Privacy Senior Associate

M: +971 50 213 4884
E: alice.gravenor@pwc.com

Digital Trust

Matt White
Partner, Head of Digital Trust

M: +971 56 113 4205
E: matt.white@pwc.com

Phil Mennie
Director

M: +971 56 369 7736
E: phil.mennie@pwc.com

www.pwc.com/m1/en/services/tax/legal-services

Established in the UAE region for 40 years, PwC has more than 4,200 people in 12 countries across the region: Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Oman, the Palestinian territories, Qatar, Saudi Arabia and the United Arab Emirates.

190205-180626-HO-OS