Meeting the Challenge of a Global GDPR and BCR Programme

John Bowman and Myriam Gufflet*

I. From Negotiation to Implementation

On 25 May 2018, the European Union General Data Protection Regulation¹ (GDPR) will be applicable in all Member States. This landmark legislation was a long time in development. The European Commission issued its draft proposal for the GDPR on 25 January 2012. It then took almost four and a half years of intensive negotiations before the Council of the European Union and the European Parliament agreed upon a final text.

It was certainly fascinating to follow the negotiations, as the different Member States in the Council and political groupings in the European Parliament attempted to fashion the GDPR in a way that reflects their own policy objectives. On the one hand, there was a desire by some negotiators to maintain the free flow of personal data in order to promote creativity, innovation and growth in the digital economy. On the other hand, privacy advocates called for stricter rules and stronger enforcement powers to reinforce the fundamental right of people in the EU to the protection of their personal data.

In the end, a compromise was reached that brought the accountability principle to the fore, provided for a risk-based approach to data-processing activities, enhanced the rights of data subjects and strengthened the powers of data protection authorities within a new cross-border regulatory framework.

As legislative discussions were finally settled, many organisations turned their attention to the practical implementation of the new rules. It has taken a significant shift in mindset to move from following the policy discussions, fascinating as they were, to taking steps to prepare for compliance with the GDPR. In this article, we describe some ways that organisations can prepare for GDPR implementation, either through a specific programme of work or through a wider privacy programme that incorporates an application for binding corporate rules (BCR).

II. How a Privacy Programme Addresses EU Requirements

When the Official Journal of the European Union published the GDPR on 27 April 2016, the two-year transition period might have seemed generous. However, many organisations have since discovered that the effort and commitment required to manage transition to the new rules should not be underestimated. As a legislative act, the GDPR has horizontal effect across organisations; GDPR implementation programmes, therefore, should address the interests and concerns of a wide range of organisations’ internal and external stakeholders. In this respect, the establishment of a privacy programme requires serious consideration and commitment from key decision-makers within an organisation.

Despite the costs of compliance with stricter data protection rules that carry higher penalties, organisations can derive substantial benefits from undertaking such a programme of work. For many, applying good data governance and effective data protection measures is about doing the right thing for their customers, employees and business partners. Organisations can therefore view the coming of the GDPR as an opportunity to take a serious look at their data processing and see what advantages they may gain through their compliance efforts.²

Large international organisations can consider applying for binding corporate rules (BCR) as a way to drive GDPR compliance within a broader privacy programme. The adoption of BCR serves a practical purpose of enabling the free flow of data within a busi-

---

* John Bowman is a senior principal, and Myriam Gufflet is a principal, both working in the privacy and data protection practice of Promontory Financial Group, an IBM Company. For correspondence: <jnbowman@promontory.com> and <mgufflet@promontory.com>.


Table 1. Territorial Scope Of GDPR and BCR

<table>
<thead>
<tr>
<th>Data origin: EEA</th>
<th>EEA</th>
<th>Non-EEA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data hosted, processed, or accessed by undertakings</td>
<td>GDPR</td>
<td>GDPR + BCR</td>
</tr>
</tbody>
</table>

| Data origin: non-EEA | GDPR | BCR may be applied to all data hosted, processed, or accessed by fully participating non-EEA undertakings |

ness group and in and out of the European Economic Area (EEA), where applicable.3

The BCR are subject to the approval of a competent data protection authority of national or EU origin, and the applicant organisation needs to demonstrate that legally binding measures are in place to protect data transferred in and out of the EEA. This arrangement replaces more cumbersome transfers of personal data across the group, such as those involving multiple sets of contractual clauses.

In a broader sense, BCR also require the applicant organisation to demonstrate that it applies general data protection principles; enables individuals to exercise their data-subject rights; and has in place various organisational measures such as complaint procedures, auditing, and training. The decision to adopt BCR subjects organisations to the scrutiny and approval of a competent EEA data protection authority, but it also allows organisations to demonstrate a high standard of cross-organisational data protection — efforts that will surely help in working towards GDPR compliance as part of a broader privacy programme.

A privacy programme configured in such a way can facilitate group-wide data transfers and support transition to the new GDPR requirements, whose broader scope will apply to:

- Data controllers and processors established in the EU that process personal data, regardless of where the data subject is located;
- Data controllers and processors not established in the EU that process personal data in the context of offering goods and services to EU data subjects, or those that monitor their behaviour.

An organisation that applies for BCR when building its privacy programme can help itself adopt a group-wide standard inside and outside of the EEA, as shown in the table above.

III. Scope and Application of BCR

The BCR are a legal mechanism enabling international transfers of personal data from EEA undertakings to non-EEA undertakings or between members of the same corporate group. The Article 29 Working Party created the BCR during the early 2000s, and the GDPR officially recognises this compliance mechanism as a valid legal transfer tool. BCR are particularly suited to multinational organisations transferring personal data globally, and data protection authorities within the EEA have approved the BCR of nearly 100 organisations.4

Organisations can decide whether to adopt controller BCR to cover their data-processing activities (including transfers) when acting as data controllers (e.g., for the purpose of managing human resources), and/or to adopt data-processor BCR when acting on behalf of clients (e.g., services offered by outsourcing providers). Given that controller BCR were created by the Article 29 Working Party a few years before

---

3 The European Economic Area comprises the 28 EU Member States, Iceland, Liechtenstein and Norway. The EEA Agreement, which created a single market, provides for the inclusion of EU legislation covering the four freedoms—the free movement of goods, services, persons and capital—throughout the 31 EEA Member States. Therefore, the GDPR will be incorporated into the EEA Agreement in the form of an annex (Annex XI ‘Electronic Communication, Audiovisual Services and Information Society’, which covers, inter alia, Data Protection).

processor BCR, most BCR adopters follow the controller variation.

Since the BCR’s creation, the Article 29 Working Party and national data protection authorities have encouraged organisations to adopt BCR privacy programmes, highlighting that they are a good way of standardising data protection processes; communicating the privacy policy of a group; and providing evidence of accountability, a key element of the GDPR.  

IV. GDPR and BCR Content

The data protection authorities’ expectations for BCR content were set forth in several opinions adopted by the Article 29 Working Party, and the vast majority of those requirements are now specified in the GDPR in Article 47.

The main differences between the Article 29 Working Party and GDPR requirements for BCR relate to the new rights and obligations introduced by the GDPR, such as the rights to data portability and to restriction of processing, and the principles of privacy by design and by default. In addition, according to Article 70(1)(i) GDPR, the European Data Protection Board is entitled to issue guidelines, recommendations and best practices to further specify BCR criteria and requirements. However, the Article 29 Working Party is already working on an update of existing opinions and reference documents on data transfers to third countries, and should issue these by the end of 2017.

There is significant overlap between the obligations placed by the GDPR on data controllers and data processors and the requirements specified for BCR:

1. Data subjects’ rights: The rights of data subjects regarding the processing of their personal data (e.g., rights of access, erasure, objection and transparency), along with the means to exercise those rights, are protected by both GDPR and BCR requirements.

2. Data handling: The general data protection principles — such as purpose limitation, data minimisation and transfers — are required by both GDPR and BCR requirements.

3. Training: Although the GDPR does not clearly require employee training (as the BCR do), it implies that data controllers and data processors should provide training to employees involved in the processing of personal data.

4. Accountability and governance: Both the GDPR and BCR require organisations to cooperate with data protection authorities and to designate a data protection officer.

5. Security and confidentiality: The GDPR and BCR both require appropriate technical and organisational measures to protect the security and confidentiality of personal data under processing.

6. Change management: GDPR and BCR requirements promote the principles of privacy by design and by default.

7. Audit and monitoring: The GDPR implies that data controllers and data processors should conduct audits of the processing operations, which BCR also require.

---

6 In particular: Article 29 Working Party, ‘Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules’ (24 June 2008) WP153; ‘Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules’ (6 June 2012) WP195.
8 Arts 12-22, 28 and 29 GDPR.
9 Art 47(2)(e) GDPR.
10 Arts 5-11 and 44-49 GDPR.
11 Art 47(2)(d) GDPR.
12 Art 47(2)(m) GDPR.
13 Art 39(1)(b) GDPR.
14 Arts 31 and 37-39 GDPR.
15 Art 47(2)(i) and (h) GDPR.
16 See Miguel Recio, ‘Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability’ (2017) 3(1) EDPL 114-118.
17 Arts 32-34 GDPR.
18 Arts 12-22, 28 and 29 GDPR.
19 Art 25 GDPR.
20 Arts 12-22, 28 and 29 GDPR.
21 Arts 5-11 and 44-49 GDPR.
22 Art 47(2)(j) GDPR.
By adopting BCR, a group can help assure internal and external stakeholders that it has set high data protection standards for its processing activities within the EEA and maintains such standards for personal data transferred to and processed by the group’s companies based in non-EEA countries. As a consequence, BCR are much more than a mechanism to legitimate transfers within a group: They constitute a proper data protection programme able to support and demonstrate compliance with the vast majority of GDPR requirements.

V. Implementation of a GDPR and BCR Programme

Given the numerous similarities between the two sets of requirements, organisations that have already implemented BCR can adapt the processes and procedures created for BCR to their GDPR compliance programmes. Likewise, organisations that have decided to simultaneously adopt BCR and prepare for GDPR compliance can rationalise their efforts and run a GDPR and BCR programme all at once and without too much additional effort.

In fact, organisations that concurrently pursue BCR and GDPR compliance will have aligned themselves with the position held by the Article 29 Working Party and by some data protection authorities — namely, that the BCR represent compliance mechanisms that reflect the notion of accountability introduced by the GDPR.23

The two sets of requirements are broadly related, even if the GDPR does not expressly cite BCR when providing examples of elements that demonstrate accountability.24 BCR are more than a tool for international data transfers, as they can serve as the backbone of an organisation-wide privacy management programme. For that reason, explicit recognition of BCR within the GDPR is a welcome development, helping promote the accountability principle, maintain legal certainty and relieve organisations of unnecessary burden.

VI. Practical Steps to Prepare for the GDPR

Whether or not organisations have already applied for and follow BCR, many have found that preparing for the GDPR takes considerable time and effort. The Article 29 Working Party is issuing guidance on the practical application of the GDPR25, but there will be no grace period for transitioning to compliance beyond the 25 May 2018 deadline. Compliance teams that adopt a wait-and-see approach on the regulatory guidance put themselves at risk — particularly if such guidance is delayed. Organisations can minimise this risk by carefully considering the GDPR text now, with the aim of fully understanding the operational impacts of working towards compliance with the new rules.

Organisations designing a GDPR gap analysis will need to take into account their size, complexity and state of compliance with current laws. The exercise itself may take several weeks to carry out, with more time required for implementation planning, identifying required resources and bidding for resources during the business-funding cycle. Building the business case for such a programme will require raising awareness among key decision-makers and influencers in an organisation, as part of an effort to win their support and sponsorship.

After a gap analysis and programme planning, GDPR implementation typically incorporates several elements:

- Initial programme setup: holding discussions with senior stakeholders, preparing a business case and budget for approval and establishing a programme governance structure;
- Scoping and planning: undertaking an initial scoping exercise and developing a plan for stakeholder management and communications;
- Information gathering: performing a document review, holding workshops and stakeholder inter-

---

24 art 24(1)(3) GDPR.
views, identifying data processes and flows, and ensuring key data controls are in place;
• Readiness assessment: mapping information gathered against a compliance framework and documenting key compliance gaps;
• Remediation planning: planning the programme, developing a remediation plan and road map, securing appropriate resources and appointing a delivery team;
• Implementation: undertaking remediation activities, implementing operational changes and transitioning to business as usual

VII. Conclusion

Many organisations starting to plan for the GDPR have taken a structured approach similar to that described above. And those that have not started planning yet should commence at the earliest opportunity.

Organisations can consider the advantages of applying for BCR concurrently with their GDPR implementation efforts. BCR are an optional extra — unlike GDPR requirements, which will be mandatory for all firms processing data in the EU. But many organisations may see the benefit of adopting a privacy programme that incorporates both the GDPR and BCR and should determine whether that approach fits within their strategic outlook for privacy and data protection as a whole.