BCRs under the GDPR: Practical considerations

Further DPA guidance is expected later this year. In the meantime, **Wanne Pemmelaar**, **Anna van der Leeuw-Veiksha** and **Charlotte Mullarkey** explain what companies should do now.

Modern businesses increasingly explore opportunities presented by their vast collections of data and depend on the free flow of this data between business units, customers and third parties. However, more and more countries are introducing stricter privacy and data protection rules (including the EU) while simultaneously establishing regional initiatives to enhance the free flow of data. At the same time, regulatory responses to rapidly developing innovative technologies and new business models that revolve around the use of data are often seen as lagging behind practice and limiting innovation. Companies operating internationally face challenges in ensuring compliance with this multitude of requirements.

As new legislation and developments shake up the existing principles of cross border data transfer, now is the time for organisations to consider the practical implications of transferring data in this new landscape. For many, Binding Corporate Rules (BCRs) are looking like an attractive option.

Why adopt BCRs?

EU data protection law generally prohibits transferring personal data outside the European Economic Area (EEA) unless the target country or territory ensures an adequate level of data protection. If this is not the case, options for compliant transfers include model contractual clauses approved by the European Commission, and BCRs.

BCRs are a set of binding rules put in place to govern intra-group data protection practices and facilitate transfers of personal data within a corporate group between the EEA and affiliates in third countries. Once approved by the EU data protection authorities (DPAs), BCRs enable the free flow of personal data within the corporate group.

BCRs provide an effective and efficient mechanism for compliance with data protection standards within a corporate group internationally. They can promote compliance with both EU and non-EU data protection laws. They also generally ensure a high level of compliance maturity and include an array of policies and procedures, audits and controls, complaints handling and training programmes. This makes BCRs a comprehensive compliance programme, rather than simply a mechanism for cross-border data transfer.

BCRs are not referred to in the existing EU Data Protection Directive but were instead developed by the Article 29 Working Party (WP29) and therefore tend to be looked on favourably by the EU data protection authorities (DPAs) as promoting real compliance. They have been formally recognised in the EU General Data Protection Regulation (GDPR) as a mechanism for cross-border data transfer. The GDPR has codified and formalised the applicable rules and the Regulation applies from 25 May 2018.

> GDPR does not differentiate between BCRs for controllers and BCRs for processors but instead provides one set of standards

The popularity of BCRs has grown immensely in the past few years, with currently over 90 companies having finalised the approval of their BCRs – half of these companies obtained their authorisations in the past three years.[1]

BCRs for Controllers and Processors

EU DPAs currently recognise two types of BCRs, with somewhat different sets of requirements and obligations: BCRs for Controllers and BCRs for Processors. BCRs for Controllers regulate personal data transfers by the organisation as data controller within the same company group. BCRs for Processors are used for international transfers of personal data that are originally processed by a processor on behalf of an EU controller and that are sub-processed within a processor's organisation.

Both types of BCRs have a similar set of provisions, however, BCRs for Processors have additional obligations that are specific to a controller-processor relationship. For instance, they must include a duty to cooperate with the controller for all members of the group, sub-processors and employees. The rules on data protection audit are much more detailed, and the audit results must be made available to the data controller. Many companies are both data controllers and data processors of personal data under EU law and could therefore benefit from both types of BCRs.

What is new in the GDPR?

One set of rules…or not? The GDPR does not differentiate between BCRs for controllers and BCRs for processors but instead provides one set of standards applicable to both types of BCR. This is in line with new obligations that processors will assume under the GDPR.

While several new requirements for BCRs are introduced by the GDPR, the full list of requirements is still considerably shorter than the current detailed criteria established by the WP29, particularly in the case of BCRs for processors. However, the European Commission may establish additional requirements and the European Data

Protection Board (EDPB) may issue guidelines, recommendations and "further necessary requirements". In practice this might mean that the EPDB will uphold the WP29 opinions on BCRs, with a risk of re-introducing administrative requirements that are simplified by the GDPR.

In the absence of official clarification, we would recommend that companies that intend to adopt BCRs seek advice from their lead authority. New WP29 guidance on BCRs is expected in the course of 2017.

"Companies engaged in joint economic activity": Until now, BCRs have been limited to arrangements among entities of the same corporate group. Under the GDPR, BCRs can be used by a group of enterprises that are engaged in joint economic activity, but are not necessarily part of the same corporate group. The GDPR leaves several practical questions open, for instance:

- what criteria will be used to define whether companies are engaged in a joint economic activity?
- which rules for selecting a lead authority will be used in cases of joint economic activity?
- may companies that are engaged in a joint economic activity already apply for BCR approval now (before the GDPR applies)?

Companies engaged in joint economic activity may choose to prepare BCR applications based on the new governance structure under the GDPR and have them take effect from 25 May 2018. If EU DPAs do not cooperate with this approach, companies will have to wait until after 25 May 2018, when the GDPR applies throughout the EU.

Minimum requirements for BCRs: The GDPR contains a list of minimum requirements which will apply to the content of BCRs. Companies that already have approved BCRs will need to amend them to the extent they do not comply. Our gap analysis of several widespread BCR models suggests that companies with BCRs will likely need to update provisions that relate to, for instance:

1. Principles of data minimisation, data protection by design and by default, and individuals' rights to restriction of processing.
2. The rules on profiling.
3. Information and transparency obligations.
4. Data security breach notification obligations.
5. Third party contracts.
6. Privacy impact assessments.
7. Provisions on data protection officers and BCR compliance mechanisms within the company group.
8. Liability for BCR breaches by any non-EU group member.
9. Mechanisms for reporting and recording of changes to the BCRs.

They will also need to think about streamlining the provisions regarding cooperation and communication with the DPAs.

Data protection officer (DPO): An obligation to create a network of privacy officers or appropriate staff for overseeing and ensuring compliance with BCRs is already required under current rules.

However, the GDPR goes further by prescribing high standards for the role and position of the DPO within an organisation. It provides specific guarantees for the DPO's independence and obliges organisations to support their DPO in executing the function. Some existing BCR implementations will deviate significantly from these requirements in terms of tasks and responsibilities.

The wording of the GDPR supports the current practice that a group of companies must designate a "person or entity" to monitor BCR compliance within the group, as well as to monitor training and handle complaints. However, appointing a DPO is not required, even for corporate groups with BCRs, unless processing activities of the group trigger mandatory designation of a DPO. The preliminary guidance on DPOs issued recently by the WP29 is consistent with this, although it does not specifically refer to BCRs.[2]

The decision of whether to combine the role for supervision and monitoring compliance with BCRs with the role of checking general compliance with the GDPR lies with the company group. Organisations with approved BCRs, or which are currently developing BCR programs, would be well advised to:

- review the position, tasks and responsibilities of the chief privacy officer under the BCRs against the DPO criteria of the GDPR;
- appoint a DPO under the GDPR for the entire company group and task this DPO with BCR-specific obligations – at least at the initial stage of BCR implementation. This will remove any ambiguity as to the position of a person responsible for BCR and contribute to creating a strong reporting line within the corporate governance structure.

Some organisations might consider splitting the roles of BCR oversight and DPO, depending on the size of the group, the group governance structure, the nature and scale of processing operations, and the complexity of data transfers etc.

Data protection audits, verification of compliance and reporting to DPAs: Having mechanisms to verify compliance with BCRs and data protection audits are not a new requirement. However, the GDPR establishes that the results of this verification should be communicated to a DPO (or another BCR monitoring entity) and to the board of the controlling undertaking of a company group or of the group of enterprises engaged in a joint economic activity. The verification results should be also made available to DPAs upon request. The GDPR further expands an obligation to record any changes to the BCRs and report those to the DPA.

In addition, the DPA should be informed of any legal requirements to which a member of the company group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the BCRs. This obligation to inform the DPA previously existed only for Processor BCRs. The scope of the reporting obligation is also expanded.

Approval process now and in the future: The current process for obtaining BCR approval is fairly straightforward and takes approximately nine months[3]. A company applies to a lead DPA and two co-lead authorities for authorisation. The lead DPA reviews the documents and, once satisfied, circulates them to other DPAs as part of a cooperation or mutual recognition procedure. Once approved, the company can apply to national DPAs for authorisations or permits for data transfers under the BCRs[4]. This long-established and well-functioning approval

mechanism seems to have been operating less smoothly in the past months. The reasons for this might include:

- low capacity at national DPAs that have to deal with the increased numbers of BCR applications, reorganisation issues resulting from their broader powers under the upcoming GDPR, or investigations of complaints;
- uncertainty at DPAs over validity of existing mechanisms for cross-border data transfers after invalidation of the EU-US Safe Harbor framework by the Court of Justice of the EU and new cases against Privacy Shield and model clauses which are pending;
- higher standards applied by the DPAs for accepting draft BCRs. For instance, companies were previously given a transition period of two years after approval of the BCR to bring all data processing operations in line, and roll out the required processes and procedures. But now the DPAs demand that the company is compliant, with all procedures in place, at the time of the application. Additionally, DPAs that were not the lead or co-lead authority now more often come up with additional questions and comments after the main application review has been completed.

What will change in the approval process under the GDPR? First of all, the GDPR introduces a definition of a lead authority – a cornerstone of the "One-Stop-Shop" mechanism. Preliminary WP29 guidance on identifying the lead DPA triggered many comments and questions and we await a revised version (this is expected by April 2017). With this in mind, the rules for selecting a lead authority for BCR authorisation, at least for group companies, will probably become less flexible. On the other hand, the new category – the group of undertakings engaged in joint economic activity - will likely be more flexible in selecting a lead DPA. We expect further guidance from WP29 this year.

Secondly, the BCR filing process under the GDPR will follow a consistency mechanism procedure. This requires the draft decision by a lead DPA to be submitted to the EDPB for a non-binding opinion adopted by simple majority of the board members. The EDPB members (representatives of all national DPAs) will review all underlying information and documentation prior to voting. This means that the lead DPA could potentially have to take on board the input of all EU DPAs. There is also a dispute resolution procedure that could further delay the BCR authorisation. Although strict deadlines and streamlined procedures are envisioned by the GDPR, this still seems a more complicated and potentially lengthy procedure than the current one.

Finally, in contrast to current practice, the GDPR does not require any further authorisations from, or notifications of, the EU DPAs for data transfers under BCRs. Under the current rules, fulfilling the different national administrative requirements presents considerable challenges in terms of resources, both in time and money. Abolishing this step is definitely beneficial to BCR applicants.

What about companies with BCRs approved under current law? The GDPR specifically provides that existing BCR authorisations shall remain valid until amended, replaced or repealed, if necessary, by the respective DPAs.

The WP29 has not set out its official position on this point, for example on the need to amend existing BCRs or to renew current authorisations. This topic was on agenda of the latest plenary meeting held on 7-8 February 2017,[5] but no details on the results were released by the date of writing.[6] Companies should look out for any new developments about current authorisations and discuss any planned changes with their lead DPA.

How will Brexit affect BCRs?

Our expectation is that BCRs issued in the EU will continue to be recognised as a data transfer mechanism that provides appropriate safeguards and enables transfers to third countries, including for transfers to and from the UK. Companies within the EU will not be affected by the outcome of the Brexit negotiations, the future of UK data protection legislation or whether the UK will qualify as providing an adequate level of protection post Brexit. BCRs are a mechanism specifically developed for enabling data transfers from the EU to countries without established adequacy of data protection and can be utilised for data transfers to any country worldwide, regardless of whether such a country even has substantive data protection laws – and thus also to the UK.

The UK government has made it clear that the GDPR will automatically apply to the UK from 25 May 2018, and the ICO is putting much work into ensuring that organisations operating in the UK are compliant with the GDPR. The UK government has also expressed its commitment to ensuring unhindered data flows after Brexit and it looks most likely that they will seek "adequate" status from the European Commission.

However, it is unclear at this point whether the UK will participate in the "One-Stop-Shop" mechanism (though this is looking increasingly unlikely) or the EDPB, and in particular in the cooperation procedure that is crucial for the authorisation and functioning of BCRs in the EEA. It is also uncertain whether the UK will maintain its role as one of the most important hubs for issuing BCR approvals[7]. We expect some form of transitional provisions will be put in place, if required, for companies with BCRs approved by the UK ICO.

REFERENCES

1 The list of companies with approved BCR can be accessed at ec.europa.eu/newsroom/document.cfm?doc_id=40100
2 See WP29 Guidelines on Data Protection Officers, available at http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf
3 See further a note on BCR at www.allenovery.com/SiteCollectionDocuments/BCRs.pdf
4 National filing requirements for controller BCR ("BCR-C"), available at ec.europa.eu/justice/data-protection/international-transfers/files/table_nat_admin_req_en.pdf
5 See ec.europa.eu/newsroom/document.cfm?doc_id=42442
6 See ec.europa.eu/newsroom/document.cfm?doc_id=42820

Main takeaways

1. Companies exporting personal data from Europe and operating internationally should think about mapping the differences between their current internal processes and procedures and requirements of the GDPR. They should also consider whether BCRs could be a key element for compliance not only with cross-border data transfers, but also for raising the overall standard of data protection in their global operations. This now also applies to businesses engaged in joint economic activity.
2. Companies that have approved BCRs should review their BCR policies and practices for compliance with the GDPR, initiate change procedures and try to engage in active dialogue with all relevant DPAs for additional guidance and clarifications.
3. Companies that have the UK ICO as their lead authority for their BCRs should engage with the ICO to discuss the best way forward to prepare for Brexit.
4. Finally, organisations that depend on data transfers to or from the UK should consider their options for compliant transfers after Brexit (including BCRs) once the position is clearer.

AUTHORS

Wanne Pemmelaar is a Senior Associate, and Anna van der Leeuw-Veiksha a Senior Professional Support Lawyer at Allen & Overy's Amsterdam office. Charlotte Mullarkey is a PSL Counsel at Allen & Overy's London office.
Emails:
wanne.pemmelaar@allenovery.com
anna.vanderleeuw@allenovery.com
charlotte.mullarkey@allenovery.com

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

UK Court of Appeal limits exemptions to access rights

Marcus Evans and **Yasmin Lilley** explain the importance of this recent court decision in the *Dawson-Damer case*.

Under the UK Data Protection Act 1998 (DP Act), data subjects have rights to obtain copies of their personal information through a data subject access request (DSAR). Data subjects frequently use DSARs to obtain information in the context of non-data protection disputes with data controllers. There has been much controversy over this practice, particularly as the £10 maximum fee the data controller may charge is a small fraction of the cost of complying with the request.

On 16 February 2017 in *Dawson-*

Continued on p.3

Data brokers beware: The ICO may be coming for you

The ICO will crack down on bad actors in the data broker industry in coming weeks. **Dugie Standeford** reports.

Data brokers are organisations which obtain data, some of which may be personal data, from various sources and then sell or license it to third parties for uses such as marketing. In 2012, data brokers' trade in personal information reportedly generated over $150 billion in revenue, Hogan Lovells' data protection attorney, Eduardo Ustaran, noted in a 16 February blog posting.[1]

The UK Information Commissioner's Office (ICO) has had data brokers in its sight for some time but will now begin monitoring them more closely, Information Commissioner

Continued on p.4

Issue 90 **March 2017**

NEWS

1 - **UK Court of Appeal limits exemptions to access rights**
1 - **Data brokers beware: The ICO may be coming for you**
2 - **Comment**
What now for data transfers?
20 - **Lack of trust: ICO asks for the consumer to be put first**

ANALYSIS

16 - **Wearables-at-work: Quantifying the emotional self**

MANAGEMENT

6 - **BCRs under the GDPR: Practical considerations**
10 - **GDPR: Time for execution**
13 - **Heart on your sleeve: The DP implications of wearable tech**
18 - **Improving data quality with end-to-end data management**
22 - **DP Impact Assessments: Challenges and recommendations**
23 - **Events Diary**

NEWS IN BRIEF

5 - **ICO consults on GDPR draft consent guidance**
5 - **UK data flows – what will the future hold?**
9 - **Government reaffirms commitment to free flow of data**
9 - **ICO calls for transparent and proportional data sharing**
12 - **DCMS prepares a UK position on e-Privacy**
15 - **New information from ICO on Big Data and AI**
23 - **ICO probes targeting of individuals in EU Referendum**
23 - **Law Commission consults on the protection of official information**

UNITED KINGDOM
report

ISSUE NO 90 **MARCH 2017**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
Glenn Daif-Burns
glenn.daif-burns@privacylaws.com

CONTRIBUTORS

Marcus Evans and Yasmin Lilley
Norton Rose Fulbright LLP

Dugie Standeford
PL&B Correspondent

Wanne Pemmelaar, Anna van der Leeuw-Veiksha and Charlotte Mullarkey
Allen & Overy LLP

Emma Fox
TLT Solicitors

Andrew McStay
Bangor University

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

What now for data transfers?

Brexit looms. But most organisations will need to transfer data across borders whatever happens. The UK government might be wise to start preparing an application to the European Commission for an adequacy decision now – the previous candidates have waited a long time to obtain their approval from the European Commission. This process has now speeded up due to a more flexible concept of "adequacy" (*PL&B International* February 2017 p.3). But will the future UK DP regime, post-Brexit, be adequate?

There is no date yet for the Investigatory Powers Act to enter into force. Its surveillance powers may not be seen as fitting with the EU DP regime, from an EU perspective. The Home Office has confirmed that in the light of the December 2016 judgement of the Court of Justice of the European Union relating to the UK's communications data regime, there will be a delay as the matter must now be considered by the domestic courts. However, the Codes of Practice relating to the Act have been published for consultation with responses invited by 6 April (www.gov.uk/government/consultations/investigatory-powers-act-2016-codes-of-practice).

One solution to transfers are Binding Corporate Rules, which are formally approved as a transfer mechanism under the GDPR. Read on p.6 practical considerations on their use. Company BCR applications are now being processed at the ICO quicker than in the past due to more staff being allocated to this task, as *PL&B* has requested.

Data controllers need to take notice of the recent Data Subject Access Request (SAR) appeal case which may affect the ICO's guidance in this area (see p.1). It is clear from our *Help!* series of Roundtables in November and January that SARs are a much bigger problem in the UK, both in terms of volumes received, and the level of detail expected in compliance compared with most EU Member States. Perhaps another area where the ICO's GDPR guidance would be welcome?

We heard the Commissioner's views on many current DP issues at the ICO's recent stakeholder conference (p.20). The regulator is now working on a new international strategy, and has recently issued draft guidance on consent under the GDPR. Organisations will face many new requirements (p. 5).

New technologies bring new data protection dilemmas with them. In this issue, read about wearable technology monitoring emotions at the workplace (p. 16) and p.13 on how wearable providers can stay within data protection law.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

4. Back Issues
Access all the *PL&B UK Report* back issues since the year 2000.

5. Events Documentation
Access UK events documentation such as Roundtables with the UK Information Commissioner and *PL&B Annual International Conferences*, in July, Cambridge.

6. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*Privacy Laws & Business* regular newsletters and website provide me with a very useful summary of legal developments on data protection issues. This is particularly valuable in the challenging area of keeping up to date on data protection law in multiple geographies. **Alan White, Pitney Bowes**"

Subscription Fees

Single User Access

UK Edition **£440 + VAT***

International Edition **£550 + VAT***

UK & International Combined Edition **£880 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-10 users. Enterprise licence for 11+ users.

Subscription Discounts

Introductory 50% discount. Use code HPSUB (first year only) for DPAs, public sector, charities, academic institutions and small and medium companies.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the International Report.
www.privacylaws.com/int