bitkom

Position Paper

Comments on Working Papers 256 and 257 on Binding Corporate Rules and Processor Binding Corporate Rules (BCRs)

17th January 2018

Federal Association
for Information Technology,
Telecommunications and
New Media

Susanne Dehmel
Mitglied der Geschäftsleitung
Recht & Sicherheit
P +49 30 27576-223
s.dehmel@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

Summary

Bitkom welcomes the update of these working papers as well as the opportunity to comment. We would like to take this opportunity to voice our concerns whether all of the obligations outlined in the working papers that have to be fulfilled by parties operating under BCRs actually have a basis in the European General Data Protection Regulation (GDPR). In addition to these concerns we think that further differentiation between different BCR constellations is needed in order to concretize the obligations outlined in the GDPR.

WP 256 and 257

1. Scope of Application and Differentiation

In Art. 47 (1)(a) GDPR two kinds of constellations are named that might operate under BCRs. One is “a group of undertakings” and the second is “a group of enterprises engaged in a joint economic activity”. The group of undertakings is defined in Art. 4 (19) GDPR as “a controlling undertaking and its controlled undertakings”. When it comes to the duty of defining the scope of application as well as the binding nature of BCRs for one of these groups it is important to notice that there isa difference betweena group of undertakings (usually easily recognizable as most often sharing the same name and corporate design) and themore or less random constellation of companies that have decided to work together closely and therefore establish BCRs. The need for a clarification who actually is comprised in and bound by the BCRs is a different one for both groups. Art. 47 (2)(a) GDPR reflects this (in the English version, unfortunately not in the German one) by saying that BCRs for a group of undertakings must contain the group´s structure and contact details and BCRs for a group of enterprises engaged in a joint economic activity must contain the structure and contact details of the group and of each of its members. This is not reflected in WP 256 on pages 3 1.1 bullet 3 and page 14 4.2 and in WP 257 3 bullet 1 and page 14 4.1 where no difference is made between the two constellations. In our view the GDPR only asks for a full list and contact details for

each member in the constellation of a group of enterprises that are engaged in a joint economic activity and not for groups of undertakings that have a controlling undertaking that is usually the point of contact for issues on the BCRs. We would welcome an adaption of the WP with regards to this difference.

We have a similar concern with the interpretation of Art. 47 (2) in WP 256 on page 3 bullet 3 and on page 14 4.1 as well as on page 3 of WP 257 (Nr. 1 bullet 1) and on page 14 4.1. Art. 47 (2) (b) seems to be interpreted in a broader way than it actually is. Art. 47 (2) (b) does not ask for a specification of the recipients in the third country or countries. It only asks for the identification of the third country or countries. We would therefore welcome an adaption to the actual text of the article in both working papers.

2.Changes to existing BCRs (WP 256 p.4 1.2/WP 257 p. 3 2.)

Art. 46 (5) GDPR explicitly states that authorizations by Member States or supervisory authorities made on the basis of Article 26(2) of Directive 95/46/EC will remain valid until amended, replaced or repealed. This is also acknowledged in the Working Papers.

It is to be welcomed, that the Art. 29 working party encourages groups of undertakings to bring their approved BCRs in line with the GDPR requirements. It is not possible to deduce from this an automatism that in any case there is a duty to report annually conducted reviews to the competent SA even if they do not lead to changes of the BCR from 25 May 2018 onwards.

It is also worth mentioning that there seems to be no legal ground for a requirement to report changes of the BCRs or the list of BCR members once a year (WP 256 page 15 point 5.1.) whether they are substantial (see WP 153 page 9 point 5.1) or not.

3.Accountability

In WP 256 page 18 6.1.2 on accountability the Art. 29 working party seems to describe an obligation for BCR members (also in third countries) to maintain a record of all categories of processing activities carried out (even if they are in a third country). This interpretation lacks a legal base in Art. 47 as no obligation to maintain a record of all categories of processing activities can be found there. The interpretation of the GDPR therefore widens the applicability of the GDPR beyond the outer borders. Due to the fact that the “principle of fairness” is not explicitly stipulated in Art. 47 sec 2 d but on page 3 of WP 256, clarification is needed how far this principle should/can apply.

WP 257

1.Complaint handling Process (2.2, page 11)

Section 2.2 Second Paragraph
We suggest to add the word "undue" so as to be consistent with the rest of the language in the GDPR:

"All BCR members shall have the duty to communicate a claim or request without ***undue*** *delay to the Controller without obligation to handle it, (except if it has been agreed otherwise with the Controller)."*

2. Data Protection Safeguards

6.1 (ii)

"On the termination of the provision of services related to the data processing, the processors and sub-processors shall, at the choice of the controller, delete or return all the personal data transferred to the controller and delete the copies thereof and certify to the controller ***upon controller´s request*** *that it has done so, unless legislation imposed upon them requires storage of the personal data transferred."*

We suggest to add "upon controller's request' as this could be read otherwise as the processor having to proactively provide a certificate of deletion. This puts an administrative burden on the processor which we believe is not necessary as the processor is already under both the legal and contractual obligation to delete. Asking a controller to send an email or a letter to the processor to obtain a certificate is not burdensome for the controller whereas putting the obligation to proactively provide such a certificate on the processor affects the latter both in terms of time and costs, especially where processors are SMEs.

6.1 (i)

"i) Transparency, fairness, and lawfulness: ~~Processors and subprocessors will have a general duty to help and assist the controller to comply with the law~~ (for instance, to be transparent about sub-processor activities in order to allow the controller to correctly inform the data subject);"

We suggest to delete the sentence stating that "processors and sub processors have a general duty to help and assist the controller to comply with the law" as the GDPR only

sets out specific instances of obligations to assist (e.g. (28 (3) (e) GDPR) but does not set out any general obligation to help and assist.

6.1 (iii)

"~~iii) Data quality: Processors and sub-processors will have a general duty to help and assist the controller to comply with the law, in particular: "~~

We suggest to delete the sentence stating that "processors and sub processors have a general duty to help and assist the controller to comply with the law" as the GDPR only sets out specific instances of obligations to assist (e.g. Art. 28 (3) (e) GDPR) but does not set out any general obligation to assist and help.

"Processors and sub-processors will execute any ~~necessary~~ ***appropriate*** *measures when asked by the Controller, in order to have the data updated, corrected or deleted. Processors and sub-processors will inform each BCR member to whom the data have been disclosed of any rectification, or deletion of data."*

We suggest deleting the notion of "necessary" and replacing it by "appropriate" instead as the notion of "necessary" going beyond what GDPR is setting out

~~*" Processors and sub-processors will execute any necessary measures, when asked by the Controller, in order to have the data deleted or anonymised from the moment the identification form is not necessary anymore. Processor and sub-processors will communicate to each entity to whom the data have been disclosed of any deletion or anonymisation of data."*~~

We suggest rephrasing this sentence. Indeed the request to anonymize the data might require new functionalities or services not covered by the processor's scope of service. In this case, the processor cannot be forced to expand the scope of service to anonymization services. The processor must be free to respond to controller by referring to the service definition set forth in the agreement that was signed between the parties and which for example states that only deletion is possible, or that the controller must use the functionalities provided within the application.

6.1 (iv)

"iv) Security: Processors and sub-processors will have a duty to implement all appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the processing as provided by Article 32 of the GDPR. Processors and sub-processors will also have a duty to assist the Controller in ensuring compliance with the

obligations as set out in Articles 32 to 36 of the GDPR taking into account the nature of processing and information available to the processor (Art.28(3)(f) of the GDPR). ~~*Processors and sub-processors must implement technical and organisational measures which at least meet the requirements of the data controller's applicable law and any existing particular measures specified in the Service Agreement.*~~ *Processors shall inform the Controller without undue delay after becoming aware of any personal data breach. In addition, sub-processors shall have the duty to inform the Processor and the Controller without undue delay after becoming aware of any personal data breach."*

We suggest to delete this sentence as this puts a general obligation on processors to be aware of and monitor any legislation whatsoever that could be applicable to any of their customers that sets out security requirements applicable to their data controller (whether telecom, banking, insurance law etc.) and goes far beyond the scope of data privacy law.