



15 February 2024

**DRAFT DECISION APPROVING PROCESSOR BINDING CORPORATE RULES
OF CERNER GROUP**

The Hessian Commissioner for Data Protection and Freedom of Information ("DE-Hessen SA"),

Pursuant to the request by Cerner Health Services Deutschland GmbH on behalf of Cerner Group, received on 16 July 2019, for approval of their Binding Corporate Rules (BCRs) for processor;

Having regard to Articles 47, 57 and 64 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR);

Having regard to the CJEU decision *Data Protection Commissioner v. Maximillian Schrems and Facebook Ireland Ltd*, C-311/18 of 16 July 2020;

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021;

Makes the following observations:

1. Article 47(1) GDPR provides that the DE-Hessen SA shall approve BCRs provided that they meet the requirements set out under this Article.
2. The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees to controllers and processors established in the EU as to the protection of personal data that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country.
3. Before carrying out any transfer of personal data on the basis of the BCRs to one of the members of the group, it is the responsibility of any data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country of destination in the case of the specific data transfer, including onward transfer situations. This assessment has to be conducted in order to determine whether any legislation or practices of the third country applicable to the to-be-transferred data may impinge on the data importer's and/or the data exporter's ability to comply with their commitments taken in the BCRs, taking into account the

circumstances surrounding the transfer. In case of such possible impingement, the data exporter in a Member State, if needed with the help of the data importer, should assess whether it can provide supplementary measures in order to exclude such impingement and therefore to nevertheless ensure, for the envisaged transfer at hand, an essentially equivalent level of protection as provided in the EU. Deploying such supplementary measures is the responsibility of the data exporter and remains its responsibility even after approval of the BCRs by the competent supervisory authority (SA) and, as such, they are not assessed by the competent SA as part of the approval process of the BCRs.

4. In any case, where the data exporter in a Member State is not able to implement supplementary measures necessary to ensure an essentially equivalent level of protection as provided in the EU, personal data cannot be lawfully transferred to a third country under these BCRs. In the same vein, where the data exporter is made aware of any changes in the relevant third country legislation that undermine the level of data protection required by EU law, the data exporter is required to suspend or end the transfer of personal data at stake to the concerned third countries.
5. In accordance with the cooperation procedure as set out in the Working Document WP263 rev.01¹, the Processor BCRs application of Cerner Group was reviewed by the DE-Hessen SA, as the competent SA for the BCRs (BCR Lead) and by two SAs acting as co-reviewers. The application was also reviewed by the concerned SAs to which the BCRs were communicated as part of the cooperation procedure.
6. The review concluded that the Processor BCRs of Cerner Group comply with the requirements set out by Article 47(1) GDPR as well as the Working Document WP257 rev.01² and in particular that the aforementioned BCRs:
 - i) Are legally binding and contain a clear duty for each participating member of the group including their employees to respect the BCRs by entering in an Intra-Group Agreement (see section 15 of the BCR-P policy, section 4 of part 2 of the application form and the Implementation Agreement);
 - ii) Expressly confer enforceable third-party beneficiary rights to data subjects with regard to the processing of their personal data as part of the BCRs (see section 24 of the BCR-P policy and page 6 of part 2 of the application form);
 - iii) Fulfil the requirements laid down in Article 47(2) GDPR:

¹ Endorsed by the EDPB on 25 May 2018.

² Endorsed by the EDPB on 25 May 2018.

- a) The structure and contact details of the group of undertakings and each of its members are described in the application form WP265 that was provided as part of the file review and in the list of entities;
- b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question are specified in sections 17, 18 and 19 of the BCR-P policy and section 8 of part 2 of the application form;
- c) the legally binding nature, both internally and externally, of the Processor BCRs is recognized in section 15 and 25 of the BCR-P policy and section 4 of part 2 as well as part 6 of the application form;
- d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the BCRs are detailed in section 8 of the BCR-P policy and section 9 of part 2 of the application form;
- e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22 GDPR, the right to lodge a complaint with the competent SA and before the competent courts of the Member States in accordance with Article 79 GDPR, and to obtain redress and, where appropriate, compensation for a breach of the BCRs which are set forth in section 16 and 21 of the BCR-P policy and section 4 of part 2 of the application form;
- f) the acceptance by the controller or processor established on the territory of a Member State of its liability for any breaches of the BCRs by any member concerned not established in the Union as well as the exemption from that liability, in whole or in part, only if the concerned party proves that that member is not responsible for the event giving rise to the damage are specified in section 20 of the BCR-P policy and page 7 of part 2 of the application form;
- g) how the information on the BCRs, in particular on the provisions referred to in points (d), (e) and (f) of Article 47(2) GDPR are provided to the data subjects in addition to Articles 13 and 14 GDPR, is specified in sections 2 and 24 of the BCR-P policy;
- h) the tasks of any data protection officer designated in accordance with Article 37 GDPR or any other person or entity in charge of

monitoring the compliance with the BCRs within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling are detailed in section 13 of the BCR-P policy;

- i) the complaint procedures are specified in section 27 of the BCR-P policy and page 8 of the application form;
- j) the mechanisms put in place within the group of undertakings for ensuring the monitoring of compliance with the BCRs are detailed in sections 12 and 13 of the BCR-P policy. Such mechanisms include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. The results of such monitoring are communicated to the person or the entity referred to in point (h) above and to the board of the controlling undertaking of the group of undertakings (in this situation to Cerner Group's headquarters, as well as to the data privacy organization) and are available upon request to the competent SA;
- k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the SAs are specified in section 7 of the BCR-P policy and section 8 of part 2 of the application form;
- l) the cooperation mechanism put in place with the SA to ensure compliance by any member of the group of undertakings is specified in section 14 of the BCR-P policy and section 6 of part 2 of the application form. The obligation to make available to the SA the results of the monitoring of the measures referred to in point (j) above is specified in 12 and 13 of the BCR-P policy;
- m) the mechanisms for reporting to the competent SA any legal requirements to which a member of the group of undertakings is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the BCRs are described in section 30 of the BCR-P policy;
- n) finally, provide for an appropriate data protection training to personnel having permanent or regular access to personal data (section 9 of the BCR-P policy and section 5 of part 2 of the application form).

7. The EDPB provided its opinion 34/2023 in accordance with Article 64(1)(f) GDPR. The DE-Hessen SA took utmost account of this opinion.

DECIDES AS FOLLOWING:

1. The DE-Hessen SA approves the Processor BCRs of Cerner Group as providing appropriate safeguards for the transfer of personal data in accordance with Article 46(1) and (2)(b) and Article 47(1) and (2) GDPR. For the avoidance of doubt, the DE-Hessen SA recalls that the approval of BCRs does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which, an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
2. The approved BCRs will not require any specific authorization from the concerned SAs.
3. In accordance with Article 58(2)(j) GDPR, each concerned SA maintains the power to order the suspension of data flows to a recipient in a third country or to an international organisation whenever the appropriate safeguards envisaged by the Processor BCRs of Cerner Group are not respected.

ANNEX TO THE DRAFT DECISION

The Processor BCRs of Cerner Group that are hereby approved cover the following:

a. Scope:

Only members of Cerner Group acting as Processors that are legally bound by the BCRs (see section 17 and 18 of the BCR-P policy and section 2 of part 1 of the application form).

b. EEA countries from which transfers are to be made:

Belgium, Germany, Finland, France, Netherlands, Spain, Ireland, Austria, Portugal, Romania, Sweden and Norway (see section 1 of part 1 of the application form and annex list of entities).

c. Third countries to which transfers are to be made:

United States of America, Canada, Chile, Australia, India, United Kingdom, Malaysia, Mexico, United Arab Emirates, Cayman Islands, Qatar, Singapore and Brazil (see section 2 of part 1 of the application form and annex list of entities).

d. Purposes of the transfer:

IT services, hosting and support for Cerner clients (see section 2 of part 1 of the application form).

e. Categories of data subjects concerned by the transfer:

Cerner client data, primarily business admin data and IT support records. Records include contact data typically of client employees. In addition,

records may include health data of client patients (see section 2 of part 1 of the application form).

f. Categories of personal data transferred:

Cerner client data, primarily business admin data and IT support records. Records include contact data typically of client employees. In addition, records may include health data of client patients contact data (see section 2 of part 1 of the application form).

APPLICATION DOCUMENTS

The following application documents form part of this draft decision:

1. Cerner BCR-P application form part 1
2. Cerner BCR-P application form part 2
3. Cerner BCR-P policy
4. Cerner BCR-P WP257 rev.01
5. Cerner BCR-P Implementation Agreement
6. Cerner BCR-P list of entities