

French Data Protection Authority - CNIL

DECISION No. 2022-016 of February 17th 2022
APPROVING CONTROLLER BINDING CORPORATE RULES OF
WEBHELP
(application for approval No. 20005804)

The “*Commission nationale de l’informatique et des libertés*”,

Pursuant to the request by WEBHELP on behalf of the group WEBHELP, received on 28 November 2017, for approval of their binding corporate rules for “controller”;

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 amended French Act No. 78-17 of January 6, 1978 relating to information technology, data files and civil liberties (the “French Data Protection Act”);

Having regard to Decree No. 2019-536 of May 29, 2019, as amended, taken for the application of the French Data Protection Act, in particular Article 73;

Following a proposal of Ms. Anne DEBET, Commissioner, and after hearing the observations made by Mr. Benjamin TOUZANNE, Government Commissioner,

MAKES THE FOLLOWING OBSERVATIONS:

1. Having regard to Article 47(1) of the GDPR, the French Data Protection Authority (the “CNIL”) shall approve Binding Corporate Rules (“BCRs”) provided that they meet the requirements set out under this Article.
2. In accordance with the cooperation procedure as set out in the Working Document WP263. Rev.01¹, the “Controller” BCRs application of WEBHELP was reviewed by the CNIL, as the competent supervisory authority for the BCRs (“BCR Lead”) and by two Supervisory Authorities (“SAs”) acting as co-reviewers. The application was also reviewed by the concerned SAs member of the European Economic Area (“EEA”) to which the BCRs were communicated as part of the cooperation procedure set up by the European Data Protection Board (“EDPB”).
3. The review concluded that the “Controller” BCRs of WEBHELP comply with the requirements set out by Article 47(1) of the GDPR as well as the Working Document WP256.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 (articles 3.1 and 3.2 of the BCRs);

¹ Endorsed by the EDPB on 25 May 2018.

² Endorsed by the EDPB on 25 May 2018.

- 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 (article 7 of the BCRs);
- iii) Fulfil the requirements laid down in Article 47(2) of the GDPR:
 - a) The structure and contact details of the group of undertakings and each of its members are described in the Application form WP264 provided as part of the review and in appendix 1 of the BCRs;
 - 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 the article 2.1 of the BCRs and in the appendix 11-A of the BCRs;
 - c) the legally binding nature of the “Controller” BCRs, both internally and externally, is recognized in article 3 of the BCRs and in article 3 of the draft Intra-Group Agreement provided for by the group;
 - 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 binding corporate rules are detailed in articles 4, 5, 6 and 11 of the BCRs;
 - e) data subjects rights in regard to the 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 of the GDPR, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79 of the GDPR, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules are set forth in articles 7 and 8 of the BCRs;
 - f) the acceptance by the controller or processor established on the territory of a Member State of its liability for any breaches of the binding corporate rules 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 article 7.2 of the BCRs;

- g) how the information on the binding corporate rules, in particular regarding the provisions referred to in points (d), (e) and (f) of Article 47.2 of the GDPR are provided to the data subjects in addition to Articles 13 and 14 of the GDPR, is specified in articles 12.1 and 12.2 of the BCRs;
- h) the tasks of any data protection officer designated in accordance with Article 37 of the GDPR or any other person or entity in charge of monitoring compliance with the binding corporate rules 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 article 9 and in the appendix 3 of the BCRs;
- i) the complaint procedures are specified in article 8 and appendix 5 of the BCRs;
- j) the mechanisms within the group of undertakings for ensuring the verification of compliance with the binding corporate rules are detailed in article 13 and appendix 7 of the BCRs. Such mechanisms include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. The results of such verification are communicated to the person or entity referred to in point (h) above and to the board of the controlling undertaking of the group of undertakings (in this situation to WEBHELP headquarters, as well as to the data privacy organization) and are made available upon request to the competent supervisory authority;
- k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority are specified in article 14 of the BCRs;
- l) the cooperation mechanism with the supervisory authority put in place to ensure compliance by any member of the group of undertakings is specified in article 12.4 of the BCRs. The obligation to make available the results of the verifications of the measures referred to in point (j) above to the supervisory authority is specified in article 13 of the BCRs;
- m) the mechanisms for reporting to the competent supervisory authority 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 binding corporate rules are described in article 12.3 of the BCRs;

- n) and, article 10 and appendix 4 of the BCRs provide for an appropriate data protection training to personnel having permanent or regular access to personal data.
4. The EDPB provided its opinion No. 02/2022 on February 7th, 2022 in accordance with Article 64(1)(f) of the GDPR. The CNIL took utmost account of this opinion.

This decision is subject to appeal before the Council of State within two months of its notification.

DECIDES AS FOLLOWS:

5. The “Controller” BCRs of WEBHELP provide appropriate safeguards for the transfer of personal data in accordance with Article 46(1), 46(2)(b) and Article 47(1) and (2) GDPR and are hereby approved.
6. However, before making use of the BCRs, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EEA law is respected in the third country of destination, including onward transfer situations. This assessment has to be conducted in order to determine if the guarantees provided by BCRs can be complied with in practice, in light of the circumstances of the possible impingement created by the third country legislation with the fundamental rights and the circumstances surrounding the transfer. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether it can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EEA.
7. 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 this BCRs. Therefore, the data exporter is required to suspend or end the transfer of personal data.
8. The approved BCRs will not require any specific authorization from the concerned supervisory authorities.
9. In accordance with Article 58(2)(j) GDPR, each concerned supervisory authority maintains the power to order the suspension of data flows to a recipient in a third country or to an international organization whenever the appropriate safeguards envisaged by the “Controller” BCRs of WEBHELP are not respected.

ANNEX TO THE DRAFT DECISION

The “Controller” BCRs of WEBHELP that are hereby approved cover the following:

- a. Scope.** These “Controller” BCRs apply where a group entity legally bound by the BCRs, and having implemented the commitments made under the BCRs, acts as a Data Controller, as well as where the entity acts as a Data Processor on behalf of WEBHELP, thus qualified as internal data processor (article 2.1 of the BCRs.)
- b. EEA countries from which transfers are to be made:** Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Italy, Latvia, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden (appendix 1 of the BCRs).
- c. Third countries to which transfers are to be made:** the transfers of personal data are made towards WEBHELP’s entities located in: Algeria, Australia, Canada, China, India, Côte d’Ivoire, Japan, Jordan, Kosovo, Madagascar, Malaysia, Mexico, Morocco, Philippines, Puerto Rico, Senegal, Singapore, South Africa, Suriname, Turkey, United Kingdom (appendix 1 of the BCRs).
- d. Purposes of the transfer:** The purposes are detailed in appendix 11-A of the BCRs. They include the following:
 - **Human resources processing activities** (e.g.: payroll and recruitment management, employee records management);
 - **Company life & services** (e.g.: IT Management, Internal Information Security);
 - **Legal & Compliance** (e.g.: Fraud prevention and detection, whistleblowing system);
 - **Operation & Marketing** (e.g.: Client and prospect leads management, WH Direct marketing campaigns);
 - **Partner & Vendor relationships:** (e.g.: Suppliers Management and Contract Management).
- e. Categories of data subjects concerned by the transfer:** Those categories are specified in appendix 11-A of the BCRs. Are included:
 - Job candidates;
 - Employees and administrators,
 - Declared relatives of employees;
 - Visitors to the premises;
 - Clients, prospective clients, business partners and business contacts;

- Attorneys;
- Suppliers and employees of suppliers.

f. Categories of personal data transferred: Those categories are specified in appendix 11-A of the BCRs.