Courtesy translation

French Data Protection Authority – CNIL

DECISION No.2023-139 of 21 DECEMBER 2023 APPROVING CONTROLLER BINDING CORPORATE RULES OF NESTLE
(application for approval No. 20005278)

The « Commission nationale de l'informatique et des libertés » (hereafter "CNIL"),

Pursuant to the request by Nestlé France SAS on behalf of the group Nestlé (hereafter "Nestlé"), 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 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;

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023;

Having regard also to the French Data Protection Act 78-17 of 6 January 1978;

On a proposal from Ms. Anne DEBET, Commissioner, and the observations made by Mr. Damien MILIC, Government Commissioner;

Makes the following observations:

1. Article 47(1) of the EU General Data Protection Regulation 2016/679 (GDPR), provides that the French Data Protection Authority (CNIL) shall approve Binding Corporate Rules (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 European Union ("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. Therefore, the data exporter commits to waive, suspend or end the transfer of personal data. 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 rev01[1], the Controller BCRs application of the group was reviewed by the CNIL, as the competent SA for the BCRs (BCR Lead) and by two Supervisory Authorities (SA) 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 Controller BCRs of the group comply with the requirements set out by Article 47(1) of the GDPR as well as the Working Document WP256 rev.01[2] 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 (article 1.1 of the BCRs and articles 2.1 and 2.2 of the intra-group 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 (article 26.2 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 that was provided as

[1] Endorsed by the EDPB on 25 May 2018.

[2] The WP256 rev.01 and WP264 are superseded by the EDPB Recommendations 1/2022. However, since the BCR-C of Nestlé had already reached the stage of a "consolidated draft" in accordance with 2.4 of WP 263 rev.01 at the time of publication of the Recommendations, it can be assessed under the previous framework, subject to the EDPB adopting its opinion by the end of 2023 (paragraph 13 of the Recommendations).

part of the file review. The list of entities is accessible on the Nestlé Group website;

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 appendix 2 of the BCRs;

c) the legally binding nature, both internally and externally, of the Controller BCRs is recognized in article 1.1 of the BCRs and articles 2.1 and 2.2 of the intra-group agreement;

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 articles 5, 6, 7, 8, 9, 10, 16, 17 and 20 of the BCRs;

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 of the GDPR, the right to lodge a complaint with the competent SA and before the competent courts of the Member States in accordance with Articles 77 and 79 of the GDPR, and to obtain redress and, where appropriate, compensation for a breach of the BCRs are set forth in articles 12, 13 and 26.2 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 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 article 27.2 of the BCRs;

g) how the information on the BCRs, in particular on 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 article 11 of the BCRs and in appendix 4;

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 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 article 23.1 of the BCRs;

i) the complaint procedures are specified in article 25 of the BCRs and in appendix 3;

j) the mechanisms put in place within the group of undertakings for ensuring the monitoring of compliance with the BCRs are detailed in article 22 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 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 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 supervisory authorities are specified in article 29 of the BCRs;

l) the cooperation mechanism put in place with the SA to ensure compliance by any member of the group of undertakings is specified in article 28 of the BCRs. 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 article 22.1 of the BCRs;

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 articles 24.4, 24.10 and 24.13 of the BCRs;

n) finally, article 21 of the BCRs and appendix 2.6 provide for appropriate data protection training to personnel having permanent or regular access to personal data ().

7. The EDPB issued opinion No 24/2023 on 16 November 2023 in accordance with Article 64(1) (f) of the GDPR. The CNIL took utmost account of this opinion.

Decides as following:

1. The CNIL approves the Controller BCRs of Nestlé 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 CNIL 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. The Controller BCR of Nestlé must be brought in line with the EDPB Recommendations 1/2022 in the framework of the 2024 annual update.

4. 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 Controller BCRs of Nestlé are not respected.

The President

Marie-Laure Denis

This decision may be subject to appeal before the Conseil d'État within a period of two months from the date of its notification.

Courtesy translation

ANNEX TO THE DECISION

The Controller BCRs of Nestlé that are hereby approved cover the following:

a. **Scope.** These "controller" BCRs apply where a BCR member legally bound by the BCRs and that implemented the commitments made under the BCRs acts as controller, as well as where the BCR member acts as a processor on behalf of the Nestlé Group, thus qualified as an internal processor (Article 1 of the BCRs).

b. **EEA countries from which transfers are to be made**: All EEA Member States (i.e., Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Liechtenstein, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden).

c. **Third countries to which transfers are to be made**: Algeria, Angola, Argentina, Australia, Azerbaijan, Bahrain, Bangladesh, Bolivia, Bosnia and Herzegovina, Burkina Faso, Cameroon, Canada, Chile, mainland China, Colombia, Democratic Republic of the Congo, Korea, Costa Rica, Cuba, Egypt, Ecuador, Ethiopia, Fiji, Gabon, Georgia, Ghana, Guatemala, Honduras, Hong Kong, United Arab Emirates, United Arab Emirates, India, United States of America, United Arab Emirates, Indonesia, Iran, Iraq, Israel, Jamaica, Japan, Jordan, Kazakhstan, Kenya, Kuwait, Lebanon, the Dominican Republic, Macedonia, Malaysia, Mali, Mauritius, Mexico, Moldova, Montenegro, Mozambique, Myanmar, Nigeria, New Zealand, Pakistan, State of Palestine, Panama, Papua New Guinea, Paraguay, Peru, Philippines, Qatar, Russia, El Salvador, Senegal, Serbia, Singapore, Sri Lanka, Switzerland, Taiwan, Tanzania, Thailand, Trinidad and Tobago, Türkiye, Ukraine, Uruguay, Venezuela, Vietnam, Yemen, Zambia and Zimbabwe. In practice, the most common third countries of destination are Switzerland, Ukraine, Brazil and the Philippines (Annex 2 of the BCRs).

d. **Purposes of the transfer:** The purposes are detailed in appendix 2 of the as follows:
   - **Administration of the undertaking** (e.g. human resources management; administration of Nestlé's IT systems; economic, financial and administrative management; business planning and reporting);
   - **Staff databases** (e.g. internal communication and facilitating interactions within the company);
   - **Recruitment** (ex: operation and improvement of recruitment targets);
   - **Management of compensation and benefits** (e.g. payroll, Compensation, Incentive Programs, Benefits and Pensions Management, Reimbursement of Expenses, Compensation Planning and Payments, Planning and Tax Compliance;
   - **IT services and information security** (e.g. provision, maintenance, support and development of Nestlé's IT systems; implementation, maintenance and improvement of information security systems and measures; investigation of IT security incidents and personal data breaches).

e. **Categories of data subjects concerned by the transfer:** Those categories are specified in appendix 2 of the BCRs. Are included:
   - Nestlé Personnel;

- Family members and other beneficiaries of Nestlé Personnel;
- Job applicants;
- Consumers, visitors to any Nestlé websites and visitors to Nestlé's premises
- Personnel of corporate Customers;
- Personnel of corporate Vendors;
- Third parties (e.g., journalists with whom Nestlé interacts from time to time);
- Participants in product development studies and clinical trials.

f. Categories of personal data transferred: Those categories are detailed in appendix 2 of the BCRs.