Courtesy translation

French Data Protection Authority – CNIL

DECISION No.2023-142 of 21 DECEMBER 2023 APPROVING CONTROLLER BINDING CORPORATE RULES OF SODEXO
(application for approval No. 20005716)

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

Pursuant to the request by SODEXO SA on behalf of the group SODEXO (hereafter "SODEXO"), 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 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 (Rule 26 of the BCRs and 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 (Rules 10 and 21 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 part of the file review;

[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 Sodexo 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).

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 8 of the BCRs;

c) the legally binding nature, both internally and externally, of the Controller BCRs is recognized in Rule 26 of the BCRs and in 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 binding corporate rules are detailed in Rules 2, 3, 4, 5, 6, 7, 8, 13 et 14 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 Rules 10, 11, 21 and 22 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 Rule 22 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 Rule 12 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 the 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 Rules 16, 17 and 20 of the BCRs;

i) the complaint procedures are specified in Rule 17 of the BCRs;

j) the mechanisms put in place within the group of undertakings for ensuring the monitoring of compliance with the BCRs are detailed in Rule 18 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 Rule 25 of the BCRs and in appendix 5;

l) the cooperation mechanism put in place with the SA to ensure compliance by any member of the group of undertakings is specified in Rule 24 of the BCRs and in appendix 4. 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 Rule 18 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 binding corporate rules are described in Rule 23 of the BCRs;

n) finally, Rule 16 of the BCRs provide for an appropriate data protection training to personnel having permanent or regular access to personal data.

7. The EDPB issued opinion No 29/2023 on 28 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 SODEXO 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 Sodexo 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 SODEXO are not respected.

Courtesy translation

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 SODEXO that are hereby approved cover the following:

a. **Scope.** Those Controller BCRs covers the processing of Personal Data by Sodexo entities established within the EEE legally bound by the BCRs when they act as controllers or as processors on behalf of another controller of the Group and to all subsequent processing of Personal Data from Sodexo entities outside Europe to any other Sodexo entities within the Group (appendix 8 of the BCRs).

b. **EEA countries from which transfers are to be made**: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Hungary, Ireland, Italy, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden (listed in the introduction of the BCRs).

c. **Third countries to which transfers are to be made**: Algeria, Australia, Brazil, Canada, Chile, China Mainland, Colombia, Costa Rica, India, Indonesia, Israel, Japan, Malaysia, Mexico, Morocco, Myanmar, New Zealand, Oman, Panama, Peru, Philippines, Republic of Korea, Singapore, South Africa, Sri Lanka, Switzerland, Thailand, Tunisia, Turkey, Uruguay, UAE, UK, USA, Venezuela, Vietnam (listed in the introduction of the BCRs)..

d. **Purposes of the transfer:** The purposes are detailed in appendix 8 of the BCRs, as follows:
   - Recruitment management;
   - Human Resources Management (including, but not limited to, administrative staff management, mobility management, work performance management, career development management, talent review training management, business travel management, active directory management etc.);
   - Accounting and financial management of employees (e.g., expenses management), suppliers/vendors, contractors/subcontractors, clients and related controls and reporting;
   - Finance, treasury and tax management (including but not limited to M&A operations, management of performance shares, financial consolidation, budgeting and forecasting solution, including reporting);
   - Risk Management (internal audit, internal controls etc.);
   - Management of employees' safety (including information and location of employees traveling or working abroad, crisis management);
   - Provision of active directory, messaging services mailbox and other IT tools or internal websites such as Sodexo's Intranet, mobile devices, and any other digital solutions or collaborative platforms;
   - IT support management, including infrastructure management, systems management, and applications;
   - Health and safety management;
   - Information security management (including, but not limited to, prevention, detection, and investigation of security incidents, monitoring of compliance with Sodexo's data security policies);

- Client relationship management, including performance of our services and any other business operations;
- Bids, sales, and marketing management;
- Supply management;
- Internal and external communication and events management;
- Data analytics operations (data analysis in order to have a better understanding and intelligence of our clients or consumers/beneficiaries, suppliers/vendors' experiences);
- Legal corporate management (including but not limited, legal entities management, management of delegations of power and authority);
- Implementation of ethics and compliance processes (in order to comply with the applicable requirements).

e. Categories of data subjects concerned by the transfer: Those categories are specified in appendix 8 of the BCRs, as follows:

- Job applicants;
- Employees;
- Former employees;
- Clients (current or potential business clients);
- Consumers/Beneficiaries (current or potential consumer/beneficiaries);
- Suppliers/vendors (business contacts);
- Contractors/subcontractors (business contacts);
- External consultants ;
- Others (visitors, site occupants, etc.).

f. Categories of personal data transferred: Those categories are specified in appendix 8 of the BCRs, as follows:

- Identification data (civil status, identity);
- Privacy (limited to leisure and other information included in CVs, emergency contact point, and information necessary for the management of the health insurance contract for all beneficiaries);
- Working life;
- CV, school, diploma, vocational training, distinctions, etc.
- Economic and financial situation (e.g. wage expectations);
- Economic and financial situation (bank details for the management of payroll);
- Connection data (e.g. credentials for authentication purposes, logs/interaction with relevant IT applications, IP address);
- Private life (private telephone number where the employee does not have a professional telephone for HLC reasons);
- Privacy (e.g. habits of life);
- Privacy (e.g. personal mail for direct marketing if the Data Subject has consented to it);
- Economic and financial situation (income, financial situation, tax situation, etc.);
- Sensitive data: food preferences or restrictions or allergies that may indirectly reveal health data or religious beliefs.