Sodexo Binding Corporate Rules

Processor Policy

Table of Contents

In this document, “Sodexo” refers collectively to the Sodexo entities who have adhered to the Processor Policy of the Binding Corporate Rules (“BCR”) by signing an intra-group agreement (“Sodexo entity” or “Sodexo entities” or “Processor Policy members”)[1].

TARGET AUDIENCE:

All Sodexo employees (including new hires and any person acting on Sodexo’s behalf such as consultants and individual contractors.

ISSUED BY:

Sodexo Group Legal Department (Global Data Protection Office)

VERSION:

1.0

REPLACES:

The Processor Policy of the Sodexo Binding Corporate Rules (“BCR”) supersedes all Sodexo data protection policies and notices that exist on the effective date to the extent they address the same issues and are not consistent with this policy.

EFFECTIVE DATE:
December 21st, 2023

In the event of any discrepancies between the English version of this Policy and a translated version, the English version will prevail.

[1] Sodexo entity or Sodexo entities means any subsidiary of the Sodexo Group (i.e., entity or entities directly or indirectly controlled by or under common control with Sodexo SA, as defined by Article L. 233-3 of the French Commercial Code) bound with the Sodexo Binding Corporate Rules.

01

General Introduction

Introduction

Sodexo has established a framework and a clear statement for Personal Data protection as part of the Sodexo Global Data Protection Compliance Program, namely the Sodexo's Binding Corporate Rules ("BCR" or "Sodexo BCR").

The Sodexo's BCR are incorporated within the Sodexo's Business Integrity Code of Conduct. Under this code of conduct, all employees are all responsible and expected to respect and protect privacy and confidential information of their stakeholders, including job applicants, employees, clients, consumers/beneficiaries, suppliers/vendors, contractors/subcontractors, and other third parties, in accordance with applicable laws and regulations.

The BCR consist of the two following policies with their appendices:

- The Data Protection Binding Corporate Rules Controller Policy ("Controller Policy" or "BCR-C");
- The Data Protection Binding Corporate Rules Processor Policy ("Processor Policy" or "BCR-P").

The Sodexo's BCR have been created to establish Sodexo's approach to demonstrate, maintain and monitor compliance with the European[2] data protection law as set out in the General Data Protection Regulation (the "GDPR")[3] across the Sodexo Group and, specifically to cross-border flows of Personal Data between the Sodexo entities.

This Processor Policy applies to all Sodexo entities and their employees (including new hires) as well as any person acting on their behalf (consultants and individual contractors) and contains 26 Rules that Sodexo must comply with and respect when collecting and processing Personal Data as a Processor and also when they transfer data to controllers or processors within the Sodexo Group.

The capitalized terms which are used in this policy are defined in Appendix 1.

The Processor Policy will be published on the website accessible at www.sodexo.com.

[2] For the purpose of these BCR, reference to Europe means the EU/EEA and Switzerland and "EU" or "European" should be construed accordingly.

[3] 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").

What is the GDPR

The GDPR gives people the right to control how their Personal Data is used.

When Sodexo collects and processes the Personal Data of Sodexo's current, past and prospective job applicants, employees, clients, consumers/beneficiaries, suppliers/vendors, contractors/subcontractors, or any third parties, this activity is covered and regulated by the GDPR.

Under the GDPR, Personal Data means any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person ("Personal Data").

Any operation or set of operations which is performed by Sodexo on Personal Data collected from Data Subjects such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction ("Processing" or "Personal Data Processing"), falls into the application of the GDPR.

GDPR distinguishes between the concepts of "controller" and "processor". The controller determines, alone or jointly with others, the purposes and the means of the Processing of Personal Data ("Controller"). The processor, on the other hand, processes Personal Data on behalf of the controller ("Processor").

Sodexo acts as a Controller in those matters in which Sodexo determines the purpose and means of processing data, and Sodexo acts as a Processor when it processes Personal Data under the documented instructions of the Controller of that data.

Does the GDPR impact cross-border data flows of Personal Data within Sodexo?

The GDPR applies not only to Sodexo entities established in the EU/EEA but also to Sodexo entities established outside of the EU/EEA if they either: (a) offer goods or services to EU Data Subjects; or (b) the Personal Data Processing which is carried out involves the monitoring of the behavior of EU Data Subjects.

The GDPR does not allow the cross-border transfers of Personal Data to countries outside Europe that do not ensure an adequate level of data protection. Some of the countries in which Sodexo operates are not regarded by the European Commission or the European Supervisory authorities as providing an adequate level of protection for fundamental rights and freedoms of natural persons in respect of processing activities.

What is the purpose and the scope of the Sodexo BCR?

The purpose of these BCR is to provide a clear statement on the protection of Personal Data in order to provide for an adequate level of protection in compliance with the provisions of the GDPR for all Data Subjects.

The Processor Policy contains 26 Rules based on, and interpreted in accordance with the GDPR, that must be followed by all Sodexo employees (including new hires and any person acting on Sodexo's behalf such as consultants and individual contractors) of the Processor Policy members when handling Personal Data, irrespective of the country in which they are located.

This Processor Policy addresses the Processing of all Personal Data of Sodexo's current, past and prospective clients, consumers/beneficiaries, as well as such Processing on behalf of a Client.

The geographical scope of the Processor Policy is the following: the Processor Policy frames all flows of Personal Data processed by Sodexo on behalf of a Client for processing activities within the Group, whatever the origin of the Personal Data.

The material scope of the Processor Policy is described in Appendix 7.

- The EU/EEA countries are the following:
  - Austria
  - Belgium
  - Bulgaria
  - Cyprus
  - Czech Republic
  - Denmark
  - Finland
  - France
  - Germany
  - Hungary
  - Ireland
  - Italy
  - Luxembourg
  - Netherlands
  - Norway
  - Poland
  - Portugal
  - Romania
  - Spain

- Sweden

- The third-party countries are the following:
  - 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

What does this mean in practice for Personal Data collected and used in Europe?

Data Subjects whose Personal Data is processed in any country by a Sodexo entity acting as a Processor and transferred within the Sodexo Group have rights to complain or obtain judicial remedies and appropriate redress and, where appropriate, receive compensation, as detailed in Rule 21 for any breach of the rules contained in the Processor Policy:

(i) which are directly enforceable against the Processor (duty to respect the instructions from the Controller, duty to implement appropriate technical and organizational security measures, duty to respect the conditions when engaging a subprocessor, duty to cooperate with and assist the Controller in complying and demonstrating compliance with the GDPR, easy access to BCR, transparency on where the legislation prevents the respect of BCR, right to complain through internal complaint mechanisms, liability and cooperation duties with Supervisory Authorities); and,

(ii) which are enforceable against the Processor in case the Data Subject is not able to bring a claim against the Controller (duty to respect the BCR, third-party beneficiary rights, liability and burden of proof with Sodexo and not the Data Subject, easy access to the BCR and transparency, complaint handling, cooperation with Supervisory Authorities, list of entities bound by the BCR, duty to cooperate with the Controller, transparency on where the legislation prevents Sodexo from complying with the BCR and Data Protection principles).

Data Protection roles

Sodexo's Group Data Protection Officer, together with the Global Data Protection Office and the network of Local Single Data Protection Points of Contact ("Global Data Protection Network) are entrusted with duties on monitoring internal compliance with the Processor Policy and any other underlying policies and procedures.

Business owners (designated as Data Protection champions in the business functions, services operations and segments), and IT applications owners are responsible for overseeing compliance with this policy by the Sodexo entities within their own perimeter and on a day-to-day basis.

Further information

Sodexo SA, as French-based multinational company, is one of the central entities of the Sodexo Group who applied, for itself and on behalf Sodexo entities of the Sodexo Group, for the approval from the competent Supervisory Authority, i.e. the French authority (Commission Nationale de l'Informatique et des Libertés or CNIL; www.cnil.fr).

If you have any questions regarding the provisions of the Processor Policy, your rights under this policy or any other data protection issues you may contact Sodexo's Group Data Protection Officer who will either deal with the matter or forward it to the relevant Local Single Data Protection Points of Contact or Business owners or IT owners within Sodexo at the following address:

Group Data Protection Officer:

e-mail: dpo.group@sodexo.com

Address:
Group Data Protection Officer
Group Legal team
Sodexo SA
255 quai de la Bataille de Stalingrad
92300, Issy-les-Moulineaux
France

The Group Data Protection Officer is responsible for ensuring that changes to this Processor Policy are notified to the Sodexo entities and to individuals whose Personal Data is processed by Sodexo via the Sodexo website at www.sodexo.com.

02

The Rules

The rules of the Processor Policy are divided into two Sections:

- Section A addresses the Data Protection Rules that Sodexo must observe when it collects and processes Personal Data.

- Section B deals with the practical commitments made by Sodexo to the European Supervisory authorities to ensure the Processor Policy bindingness and effectiveness.

Section A

RULE 1 - COMPLIANCE WITH THE BCR, THE GDPR AND APPLICABLE LOCAL LAW

RULE 1.A - Sodexo complies first and foremost with the provisions of the Processor Policy, set out in accordance with the GDPR and applicable local law, that would require a higher level of protection for Personal Data, where it exits.

Sodexo complies with the provisions of the Processor Policy, set out in accordance with the GDPR and applicable local law where it exits.

Where the applicable local law requires a higher level of protection for Personal Data than the GDPR, such applicable local law takes precedence over the Processor Policy.

Where there is no specific law or where this law does not meet the standards set out by the BCR, Sodexo's position is to process Personal Data adhering to the Processor Policy.

RULE 1.B - Sodexo cooperates and assists Controllers to comply with their obligations under the GDPR and applicable local law, if any, that would require a higher level of protection for Personal Data, in a reasonable time and to the extent reasonably possible.

Sodexo, within a reasonable time and to the extent reasonably possible, as required under its contractual obligations or other binding documents with a Controller (a Client), co-operates with and assists the Controller (a Client) in the Controller's efforts to comply with the GDPR and applicable local law.

RULE 2 - ENSURING LAWFULNESS, FAIRNESS AND TRANSPARENCY

RULE 2.A - Sodexo assists the Controller to comply with its obligations of lawfulness, fairness and transparency.

Sodexo provides assistance to the Controller (a Client) upon request.

Sodexo also assists and cooperates with the Controller to respond to Data Subject's requests and complaints (see Rules 25 and 17), to inform the other parties involved in the Personal Data Processing as appropriate so that Data Subjects' Personal Data is accurate and kept up to date (see Rule 5) and to reply to any investigation or inquiry from the Supervisory Authorities.

RULE 2.B – Sodexo collects and processes Personal Data only on behalf and in accordance with the instructions of the Controller.

Sodexo only collects and processes Personal Data on behalf of and in accordance with (lawful) documented instructions received from the Controller (a Client), as specified in the service agreement, contract and any other binding document with the Controller (a Client).

If Sodexo is unable to comply with this Rule, Sodexo promptly informs the Controller. In such case, the Controller is entitled to terminate the contractual relationship with Sodexo to the extent related to the Personal Data Processing, subject to the conditions set out in the service agreement, contract or any relevant other binding document with the Controller (a Client). If the Personal Data Processing conditions are likely to change during the performance of the services provided by Sodexo, Sodexo informs the Controller who will have the possibility to object to the change or to terminate the contract or any other binding document concerned prior to the implementation of such change.

RULE 3 - ENSURING PURPOSE LIMITATION

RULE 3 - Sodexo processes Personal Data on behalf of the Controller for a known, relevant and legally grounded purpose determined by the Controller.

Personal Data is processed by Sodexo on behalf of the Controller, for specified, explicit and legitimate purposes as instructed by Controller and not further processed in a manner that is incompatible with those purposes, including regarding transfers of Personal Data to a third country, unless required to do so by GDPR or applicable local law to which Sodexo as Processor

is subject and that requires a higher level of protection for Personal Data. In such a case, Sodexo informs the Controller of that legal requirement before the processing takes place, unless the law prohibits such information on important ground of public interest. In other cases, if Sodexo as a Processor cannot provide such compliance for whatever reasons, it agrees to inform promptly the Controller of its inability to comply, in which case, the Controller is entitled to suspend the transfers of Personal Data at stake and/or terminate the contract or any other binding document.

RULE 4 - ENSURING DATA MINIMIZATION

RULE 4 - Sodexo processes only Personal Data which is relevant and required for the performance of the services.

Sodexo identifies the minimum amount of Personal Data that is required in order to properly fulfil the purposes of the services as set out in the service agreement, contract and any other binding document entered into with the Controller (a Client).

RULE 5 - ENSURING ACCURACY

RULE 5 - Sodexo assists the Controller to keep Personal Data accurate and, where necessary, up to date.

Sodexo and its subprocessors (if any) act upon the instructions of the Controller (a Client) in order to assist the Controller to comply with its obligation to keep Personal Data accurate and, where necessary, up to date, in order to have the Personal Data updated, corrected or deleted.

Sodexo, acting as a Processor, informs each Sodexo entity to whom the Personal Data has been disclosed of any rectification or deletion of Personal Data.

When required to do so, upon instruction from a Controller, as required under the provisions of its contract or other binding document with that Controller, Sodexo and its subprocessors (if any) shall execute the necessary measures in order to have the Personal Data deleted or anonymized from the moment the identification form is not necessary anymore.

Sodexo, acting as a Processor, informs each Sodexo entity to whom the Personal Data has been disclosed of any deletion or anonymization of data.

RULE 6 - ENSURING STORAGE LIMITATION

RULE 6 - Sodexo assists the Controller to keep Personal Data for as long as necessary.

Personal Data is always kept and/or erased and/or anonymized under the instructions of the Controller (provided such instructions do not conflict with applicable local laws) and in line with the Sodexo Global Data Collection and Data Retention Policy (Appendix 2). Sodexo disposes of Personal Data only in a secure manner in accordance with the Group Information & Systems Security Policy[4].

On termination of the provision of the services relating to the Personal Data Processing, Sodexo as Processor and its subprocessors (if any), at the choice of the Controller, delete, anonymize or return all the Personal Data transferred and the copies thereof to the Controller that it has done so, unless applicable local law, for instance EU/EEA legislation, requires storage of the Personal Data transferred. In that case, Sodexo informs the Controller and warrants that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.

RULE 7 - TAKING APPROPRIATE TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

RULE 7.A - Sodexo adheres to the Sodexo Group Information & Systems Security Policy and puts in place the technical and organizational measures as specified in the service agreement, contract and any other binding document with the Controller in compliance with the Controller's applicable local law.

Sodexo complies with the requirements contained in the Sodexo Group Information & Systems Security Policy[5] as revised and updated from time to time, together with any other security, integrity and confidentiality measures relevant to a business area or function as well as with technical and organizational security measures specified in the contract or any other binding document with the Controller (a Client) that will protect Personal Data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access, in addition to the Controller's applicable local law.

[4] Internal document

[5] Internal document

Depending on the nature of the Personal Data Processing, these technical and organizational measures may include encryption of the Personal Data, on-going reviews of security measures, redundancy and back-up facilities, and regular security testing.

RULE 7.B - Sodexo appoints a subprocessor within the Group or externally with the prior general or specific written authorization of the Controller and according to commitments similar to those set out in the contract with the Controller and in the Processor Policy.

Sodexo ensures that the subprocessing of Personal Data within the Group and/or onward transfers to external subprocessors, are performed with the prior general or specific informed written authorization of the Controller in accordance with its instructions (e.g., general or specific authorization, notification of change, possibility to object any change or terminate the contract) with regard to the appointment of subprocessors as set out under the provisions of the service agreement, contract or any other binding document and is strictly relevant to the purpose of the performance of the services.

In case of subprocessing within the Group, Personal Data may be subprocessed by other Sodexo entities bound by the BCR only with the prior informed[6] specific or general written authorization of the Controller.

Sodexo ensures that up-to-date information regarding its appointment of subprocessors is available to the Controller in accordance with the contractually agreed instructions of the Controller.

Where the Controller agrees to the appointment of subprocessors, those subprocessors will be appointed according to commitments similar to those set out in the contract between Sodexo and the Controller, and in any case in accordance with Rule 7.B and the Processor Policy.

RULE 7.C - Sodexo notifies any Personal Data Breach to the Controller without undue delay in accordance with the conditions agreed under the contract or any other binding document.

Sodexo notifies any Personal Data Breach to the Controller within the period of time agreed with the Controller of becoming aware of it and in any case without undue delay.

Sodexo assists the Controller in the identification of the nature of the Personal Data Breach, the likely consequences of the Personal Data Breach, the measures to be proposed or to be taken to address the Personal Data Breach and with any other requests of assistance from the Controller in accordance with the contractually agreed instructions of the Controller.

[6] Information on the main elements (parties, countries, security, guarantees in case of international transfers, with the possibility to get a copy of the contract used).

In addition, the subprocessors (if any) have the duty to inform Sodexo acting as a Processor as well as the Controller without undue delay.

RULE 7.D - Sodexo ensures that Personal Data processed on behalf of the Controller is kept confidential.

Sodexo ensures that any Personal Data that it processes is kept confidential.

Sodexo ensures that all persons authorized to process the Personal Data are committed to comply with an appropriate obligation of confidentiality.

RULE 8 - SAFEGUARDING THE USE OF SENSITIVE PERSONAL DATA AND OTHER SPECIAL CATEGORIES OF PERSONAL DATA

RULE 8 - Sodexo processes the Sensitive Personal Data and other special categories of Personal Data only in compliance with the Controller's lawful written and documented instructions and do not further process such data for other purposes.

Sodexo processes Sensitive Personal Data and other Special Categories of Personal Data only in compliance with Controller's lawful instructions and do not further process them for other purposes.

If Sodexo cannot process such Personal Data in compliance with the Controller's instructions, it promptly informs the Controller of its inability to comply, in which case, the Controller will be entitled to terminate the contractual relationship with Sodexo while complying with the instructions of the Controller regarding the return, the anonymization and the destruction of Personal Data in accordance with Rule 6.

RULE 9 - KEEPING RECORDS OF DATA PROCESSING ACTIVITIES

RULE 9 - Sodexo keeps records of all categories of processing activities carried out on behalf of the Controller.

Sodexo keeps records of its processing activities performed on behalf of the Controller, including a general description of the security measures implemented in respect of the Personal Data processed on behalf of the Controller.

These records include, in accordance with Article 30(2) of the GDPR the following:

(i) the name and contact details of the Sodexo entity acting Processor and of each controller on behalf of which the Sodexo entity is acting, and of the Data protection officer;

(ii) the categories of processing carried out on behalf of each Controller;

(iii) where applicable, cross-border transfers of Personal Data to a third country, including the identification of that third country and, in the case of transfers to third-party countries that are no recognized as adequate countries, the documentation of suitable safeguards;

(iv) where possible, a general description of the technical and organizational security measures referred to in Article 32(1) of the GDPR, to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a. the pseudonymization and encryption of Personal Data;

b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Upon request, these records will be disclosed to the relevant Supervisory Authorities or to the Controller.

Sodexo as a Processor makes available to the Controller all information necessary to demonstrate compliance with their respective obligations and allows for and contributes to audits, including inspections conducted by the Controller or another mandated by the Controller. In

addition, Sodexo immediately informs the Controller if in its opinion any instructions infringe the GDPR or any other applicable local law.

RULE 10 - HONOURING DATA SUBJECTS RIGHTS

RULE 10 - Sodexo assists the Controller to respond to the Data Subjects' Rights.

The Sodexo and its subprocessors (if any) execute any appropriate technical and organizational measures, insofar as this is possible, when asked by a Controller, for the fulfillment of the Controller's obligations to respond to requests for exercising the Data Subjects rights, including, to the extent legally permitted by EEA/EU legislation, by promptly notifying the Controller if it receives a request from a Data Subject for access to, rectification, erasure, restriction, portability, objection to that individual's Personal Data Processing.

Sodexo does not respond to any such Data Subject request without the Controller's prior written consent.

Sodexo provides the Controller with cooperation, assistance and useful information in relation to a Data Subject's request in order to help the Controller to comply with the duty to respect the rights of the Data Subjects, to the extent legally permitted and to the extent the Controller does not have access to such Personal Data through its use for the services provided by Sodexo or its subprocessors (if any).

If Sodexo has been instructed by the Controller to provide a generic email address to allow the Data Subjects to exercise their rights, Sodexo could be further directly contacted by the concerned Data Subjects, provided that the Controller has provided the relevant information to the Data Subjects in accordance with the GDPR.

The Data Subject has the right to lodge a complaint with the Supervisory Authority and to lodge a complaint to the courts in accordance with Rule 17 of the Processor Policy.

RULE 11 - COMPLYING WITH AUTOMATED INDIVIDUAL DECISION-MAKING AND PROFILING CONDITIONS AND IMPLEMENTING THE SUITABLE SAFEGUARDS

Rule 11 is not applicable to Processors.

RULE 12 - TRANSPARENCY AND DATA SUBJECT'S INFORMATION

RULE 12 - Sodexo makes the Processor Policy readily available to the Controller.

The Processor Policy is made available to the Data Subjects on the Sodexo's official website. In addition, the Global Data Protection Policy (Appendix 5) includes a dedicated schedule on the third-party beneficiary rights.

The Processor Policy is also available and enforceable to the Controller as it will be included by reference in the data processing agreements entered into with the Clients or any other binding document. The data processing agreement or any other binding document entered into with the Clients contains (i) the commitment of the Controller that if the transfer involves special categories of data, the Data Subject has been informed or will be informed before the transfer that his data could be transmitted to a third country not providing adequate protection; (ii) the commitment of the Controller to inform the data subject about the existence of processors based outside of EU and of the BCR; (iii) the commitment of the Controller to make available to the Data Subjects upon request a copy of the BCR and of data processing agreement or any other binding document.

RULE 13 - ENSURING ADEQUATE PROTECTION FOR CROSS TRANSFERS OF PERSONAL DATA

RULE 13 - Sodexo does not transfer Personal Data to third parties outside the EU/EEA without ensuring adequate protection for the Personal Data transferred.

When the transfer of Personal Data is made to a third party, the Sodexo entity transferring the Personal Data as Processor:

- obtains the Controller's prior consent for such transfer to a third party;
- ensures in a written service agreement, contract or any other binding document such as a data processing agreement with the third party that said third party commits in writing to provide sufficient guarantees in compliance with GDPR and the EDPB guidelines;

- signs module 3 of the European Commission standard contractual clauses[7] (transfers between Processors), and if necessary, implements supplementary measures as needed in accordance with Schrems II.

RULE 14 - EMBRACING PRIVACY BY DESIGN AND BY DEFAULT

RULE 14 - Sodexo assists the Controller in implementing appropriate technical and organizational measures to comply with data protection principles and facilitate privacy by design and by default.

Sodexo assists the Controller in implementing appropriate technical and organizational measures to comply with data protection principles and facilitate privacy by design and by default

RULE 15 - CONDUCTING DATA PROTECTION IMPACT ASSESSMENT (DPIA)

RULE 15 - Sodexo assists the Controller to conduct the required Data Protection Impact Assessments.

In accordance with Articles 35 and 36 and Recital 95 of the GDPR, Sodexo provides a reasonable assistance as set forth in the service agreement, contract or any other binding document with the Controller to make available the information related to the Processing of Personal Data it handles on behalf of the Controller, to ensure the Controller's compliance with the obligations deriving from the carrying out of DPIAs and from prior consultation of the supervisory authority, where necessary and upon request.

[7] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

Section B

RULE 16 - TRAINING AND AWARENESS

RULE 16 - Sodexo provides training to employees who have permanent or regular access to Personal Data and/or who are involved in the collection of Personal Data or in the development of tools used to process Personal Data on behalf of the Controller.

A comprehensive training program

To make the Processor Policy enforceable and effective, the Global Data Protection Office has implemented a comprehensive training program which explains the principles governing the Processing of Personal Data under this Policy.

A general module is intended to provide foundational training materials on Data Protection principles to all Sodexo employees whereas specific modules are intended for Sodexo entities' employees who have permanent or regular access to Personal Data and/or are involved in the collection of Personal Data or in the selection or development of tools used to process Personal Data. In addition, employees within a Sodexo entity should be made aware of their obligations to comply with Sodexo Data Protection policies under the Sodexo Business Integrity Code of Conduct[8].

The modules are updated regularly to better reflect Sodexo's activities and make employees understand how to deal with Personal Data protection in their day-to-day professional life.

In addition, Local Single Data Protection Points of Contact provides training in compliance with local law taking into account their specific requirements.

Monitoring of the training program

Sodexo entities take reasonable and appropriate steps to communicate with their employees and to provide appropriate training on the requirements of the Processor Policy.

Completion of the Data Protection training program is monitored by the Global and Local Single Data Protection Points of Contact together with the Global and the Local Learning and Development teams.

[8] Internal Document

RULE 17 - DATA PROTECTION RIGHTS HANDLING

RULE 17 - Sodexo assists the Controller to respond to a request or complaint it received.

When a Local Single Data Protection Point of Contact receives a request from a Data Subject or a complaint from the Supervisory Authority that relates to Personal Data Processing carried out on behalf a Controller, it is her/his role to communicate it to the Controller concerned without undue delay (or within the notification period of time agreed with the Controller) and without obligation to handle it (unless the Controller has instructed Sodexo to handle it).

The role of the Local Single Data Protection Point of Contact is to handle requests from Data Subjects and complaints from Supervisory Authorities only upon instructions of the Controller or if the Controller has disappeared factually or has ceased to exist in law or has become insolvent.

If the Controller has disappeared factually or has ceased to exist in law or has become insolvent, Sodexo handles the request without undue delay and in any event within one month after receiving the request, or if necessary, due to the complexity and the number of the requests within the extended period of 3 months (1 + 2) maximum, after informing the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay, in accordance with Article 12(3) of the GDPR. If the request was made by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

In such case, the Data Subjects are informed about practical steps of the requests and complaints handling system in the local data protection policies implementing the Global Data Protection Rights Management Policy set out in Appendix 6.

RULE 18 - ASSESSMENT OF COMPLIANCE: AUDIT PROGRAM

RULE 18 - Sodexo responds to Controllers' audit requests.

According to the Sodexo Global BCR Audit Program, Sodexo audits the Sodexo Group's compliance with the Processor Policy, and in particular implements an audit plan which covers all aspects of the Processor Policy including methods of ensuring that corrective actions will take place.

The Sodexo audits are carried out annually by the Internal Control team and also by the Group Internal Audit team as needed on specific request from the Group Data Protection Officer.

The internal auditors can be assisted by external auditors, when needed.

The results of all audits should be communicated to the Group Data Protection Officer and to the Local Single Data Protection Points of Contact and to Sodexo's Group Board of Directors and relevant members of the Group executive committee.

Corrective actions are decided on the basis of the report.

Sodexo allows the relevant Supervisory Authorities to access the results of the internal audits upon request and to carry out a Data Protection audit of any Sodexo entity if required.

Sodexo responds to Controllers' audit requests as agreed in service agreements, contracts or any other binding document entered into with Controllers.

Sodexo entities acting as Processors or their subprocessors accept, at the request of the Controller, in writing, to submit their data processing facilities for audit of the processing activities relating to that Controller which can be carried out either by the Controller or by an inspection body composed of independent members and in possession of the required professional qualifications, bound by a duty of confidentiality, selected by the Controller, where applicable, in agreement with the Supervisory Authority.

RULE 19 - MONITORING OF BCR APPLICATION

RULE 19 - Sodexo monitors the BCR application.

To ensure the Processor Policy effective implementation, the Global Data Protection Office has established a risk register.

In addition, each Local Single Data Protection Point of Contact reports local best practices in the implementation of the Processor Policy as well as Data Protection Impact Assessments carried out locally to the Global Data Protection Office, on quarterly basis. The reports of the Data Protection Points of Contact are centralized and analyzed by the Global Data Protection Office. The results of the analysis are part of the annual report provided to the Sodexo's Executive Committee.

RULE 20 - GLOBAL DATA PROTECTION OFFICE AND NETWORK OF LOCAL SINGLE POINTS OF CONTACT

RULE 20 - Sodexo ensures compliance with the Processor Policy through a Data Protection Governance structure.

To oversee and ensure compliance with the Processor Policy, Sodexo has implemented with the support of Sodexo's Executive Committee, a Data Protection Governance structure as follows:

- a Group Data Protection Officer designated in line with Article 37 of the GDPR reporting to the Group General Counsel;
- a Global Data Protection Office composed of Group Data protection counsels at the global level, supporting the Group Data Protection Officer in their tasks;
- a network of Local Single Data Protection Points of Contact ("Local DP SPOC") at the local level.

The Group Data Protection Officer's role is to monitor compliance at a global level and assess the Sodexo Data Protection program effectiveness (collection of information to identify processing activities, analysis and verification of the compliance, etc.). The Group Data Protection Officer provides the senior management with advice and recommendations as well as annual report of the Global Data Protection Office's activities. In addition, the Global Data Protection Office's role is to monitor compliance at global level and assesses the Sodexo Global Data Protection Compliance Program effectiveness.

The Group Data Protection Officer advises and supports the Local DP SPOCs when needed to comply with the Sodexo Global Data protection Program, deal with Supervisory Authorities' investigations, and ensure that the Local DP SPOC's role of handling local complaints from Data Subjects in accordance with Rule 17, of reporting major Data Protection issues to the Group Data Protection Officer, of ensuring compliance at a local level and of being accessible, in local language, to the local Data Subjects, the Controller (a Client) and to the local Supervisory Authority, is fulfilled.

RULE 21 - THIRD-PARTY BENEFICIARY RIGHTS

RULE 21 - Sodexo confers expressly rights on Data Subjects either when those rights are directly enforceable against Sodexo or when rights are enforceable against Sodexo in case the Data Subject is not able to bring a claim against the Controller.

1. **Rights which are directly enforceable against Sodexo as Processor**:

The Data Subjects are able to enforce the Processor Policy against the Sodexo entities acting as Processors and in particular:

- **Duty to respect the instructions from the Controller regarding the Personal Data Processing, including for transfers of Personal Data to third countries**;

- **Duty to implement appropriate technical and organizational security measures and duty to notify any Personal Data Breach to the Controller** (Rule 7);

- **Duty to respect the conditions when engaging a subprocessor either within or outside the Group** (Rule 7);

- **Duty to cooperate with and assist the Controller in complying and demonstrating compliance with the law such as for answering requests from Data Subjects in relation to their rights** (Rules 1B, 2A, 5, 10, 17 and 23);

- **Transparency on the Processor Policy**: Data Subjects have easy access to their third-party beneficiary rights since the Processor Policy is made available on Sodexo's Intranet and official website. They may obtain a copy of this policy from the BCR members acting as Processors upon request. In addition, the Global Data Protection Policy (Appendix 5) includes a dedicated schedule on the third-party beneficiary rights.

- **Transparency on where national legislation prevents Sodexo Group from complying with the BCR**: They may enforce Rule 23.

- **Right to Complain**: When a Local Single Data Protection Point of Contact receives a complaint from a Data Subject that relates to Personal Data Processing carried out on behalf of a Controller, he/she will communicate it to the Controller concerned without delay to the Controller without obligation to handle it. The Local Single Data Protection Point of Contact handles complaints from this Data Subject only upon instructions of the Controller or if the Controller has disappeared factually or has ceased to exist in law or has become insolvent. In such case, the Data Subjects are informed about practical steps of the complaint system in the local data protection policies implementing the Global Data Protection Rights Management Policy set out in Appendix 6. The Data Subjects are informed about: (i) where to complain; (ii) in which form; (iii) the timescale for the reply on the complaint; (iv) consequences in case of

rejection of the complaint; (v) consequences in case the complaint is considered as justified; (vi) right to lodge a claim before the Court or relevant Supervisory authority.

- **Cooperation**: Data Subjects may enforce Rule 24.

- **Liability**: Sodexo SA, as EU headquarters of Sodexo acting as Processor, accepts responsibility for and agrees to take the necessary actions to remedy the acts of other Sodexo entities established outside EU/EEA or breaches caused by external subprocessor established outside EU/EEA, to pay compensation for any damages resulting from a violation of the BCR or to demonstrate that such Sodexo entities established outside EU/EEA are not responsible for the breach or that the breaches causes by external subprocessor did not take place. The abovementioned Sodexo SA who has accepted liability shall have the burden of proof to demonstrate that the Sodexo entity outside the EU/EEA is not liable for any violation of the rules which has resulted in the Data subject claiming damages. If it can prove that the said Sodexo entity is not responsible for the event giving rise to the damage, it may discharge itself from any responsibility.

2. **Rights which are enforceable against Sodexo as Processor in case the Data Subject is not able to bring a claim against the Controller**:

Data Subjects covered by the scope of the Processor Policy are third party beneficiaries by virtue of this third-party beneficiary Rule within the Processor Policy which is given a binding effect by the intra-group agreement signed between the entities of the Sodexo Group.

To be enforced by the Controller, the Processor Policy will be included in the service agreement, contract or any other binding document signed between a Sodexo entity acting on behalf of a Controller and said Controller (a Client).

Data Subjects are entitled to enforce compliance with the Processor Policy against the Controller on behalf of which Personal Data is processed by Sodexo by lodging a complaint before the relevant Supervisory Authority or before a competent court for the EU/EEA Controller.

However, Data Subjects may enforce the Rules set out in the Processor Policy as third party beneficiaries where they are not able to bring a claim against the Controller in respect of a breach of any of the commitments in the Processor Policy by a Sodexo entity (or by a subprocessor) acting as a Processor (for example in case the Controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the Controller by contract or by operation of law, in which case the Data Subjects can enforce their rights against such entity).

In such as case, Data Subjects may at least enforce the following rules contained in the Processor Policy:

- Duty to respect the BCR (Rule 1);
- Third-party beneficiary rights (Rule 21);
- Liability and burden of proof with Sodexo and not the Data Subject (Rule 22);

- Easy access to the BCR and transparency (Rule 12);
- Complaint handling (Rule 17);
- Cooperation with Supervisory Authorities (Rule 24);
- Transfers of Personal Data (Rule 13);
- List of entities bound by the BCR;
- Duty to cooperate with the Controller (Rule 1);
- Transparency, fairness and lawfulness (Rule 2);
- Purpose limitation (Rule 3);
- Data quality (Rule 4, 5 and 6);
- Security (Rule 7);
- Data Subject's rights (Rule 10);
- Sub processing (Rule 7B);
- Transparency where national legislation prevents the group from complying with the BCR (Rule 23).

3. Compensation and jurisdiction provisions (for both Data Subjects' rights abovementioned in 1. and 2.)

Data Subjects may lodge a complaint (i) with the French Supervisory authority (the "Commission Nationale de l'Informatique et des Libertés", the "CNIL") against Sodexo SA responsible for exporting the data (a) with the Supervisory authority in the Member State of their habitual residence, (b) their place of work or (c) the place of the alleged infringement and ii) before the French competent courts where Sodexo SA has its headquarters or before the competent courts of the EU/EEA Member States where they have their residence. Where Sodexo as a Processor and the Controller involved in the same Processing of Personal Data are found responsible for any damage caused by such processing, the Data Subjects are entitled to receive compensation for the entire damage directly from Sodexo acting as a Processor.

RULE 22 - LIABILITY

RULE 22 - Sodexo complies with the following rules on liability.

Where a Data Subject suffers from damage as a result of the Processing of Personal Data by Sodexo in non-compliance with the Processor Policy, the Controller retains the responsibility to comply with the GDPR. Controllers who fall into the scope of the GDPR will pass certain Data Protection obligations on to Sodexo in the service agreements, contracts or other binding documents Sodexo has with them. Consequently, if Sodexo fails to comply with the Controller's instructions regarding the Personal Data Processing as set out in the service agreement, contract or other binding document it enters into with a Controller, the Controller may be in breach of the

GDPR and the contract and Sodexo may face a claim for breach of contract, which may result in the payment of compensation for any material or non-material/distress damages or other judicial remedies.

In such cases, if a Controller demonstrates that it has suffered damage, and that it is likely that the damage has occurred due to a breach of the Processor Policy by a Sodexo entity outside Europe (or a third party subprocessor established outside Europe), that Controller is entitled to enforce the Processor Policy against Sodexo SA, as EU headquarters of Sodexo.

Sodexo SA will accept responsibility for and agrees to take the necessary actions to remedy the acts of other Sodexo entities established outside EU/EEA or breaches caused by external subprocessor established outside EU/EEA, to pay compensation for any damages resulting from a violation of the BCR or to demonstrate that such Sodexo entities established outside EU/EEA are not responsible for the breach or that the breaches caused by external subprocessor did not take place. In addition, Sodexo SA will have the burden of proof to demonstrate that the Sodexo entity outside the EU/EEA is not liable for any violation of the rules which has resulted in the Data Subject claiming damages. If it can prove that the said Sodexo entity is not responsible for the event giving rise to the damage, it may discharge itself from any responsibility.

03

Final Provisions

RULE 23 - ACTIONS IN CASE OF NATIONAL LEGISLATION OR PRACTICES PREVENTING RESPECT OF BCRS - LEGALLY BINDING REQUEST FOR DISCLOSURE OF PERSONAL DATA

RULE 23.A - Sodexo conducts an assessment of applicable local law and practices before any transfer of Personal Data to ensure that they do not prevent it from fulfilling its obligations under the Processor Policy and have a substantial effect on its ability to comply with this policy.

RULE 23.B - Sodexo ensures that where it has reason to believe that the applicable local law or practices prevent it from fulfilling its obligations under the Processor Policy and have a substantial effect on its ability to comply with this Processor Policy, it promptly informs the Controller and/or Sodexo SA or the EU/EEA BCR member or the Group Data Protection Officer and any other relevant Local Single Data Protection Point of Contact and the Sodexo entity acting as Data Exporter.

RULE 23.C - Sodexo ensures that where it receives a legally binding request for disclosure of Personal Data which is subject to the Processor Policy, it notifies promptly Sodexo SA, the Group Data Protection Officer, the Sodexo entity acting as Data Exporter, the Controller (through the Sodexo entity acting as Data Exporter), and where possible, the data subject if instructed by the Controller, unless prohibited from doing so by a law enforcement authority; and puts the request on hold unless prohibited from doing so by a law enforcement authority or agency. The notification will include, amongst others, information about the data requested, the number of requests, the requesting body and the legal basis for the disclosure.

Assessment of the applicable local law and practices

In accordance with the EDPB recommendations[9] and the European Union Standard Contractual Clauses[10]:

Sodexo entities warrant that they have no reason to believe that the applicable local law and practices prevent them from fulfilling their obligations under the Processor Policy or their contractual obligations with the Controller and have a substantial effect on their ability to comply with this policy or their obligations. This is based on the understanding that applicable local laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR, are not in contradiction with the Processor Policy.

[9] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of Personal Data adopted on 18 June 2021.

[10] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

Sodexo declares that in providing this warranty it has taken due account, with the assistance of the Group Data Protection Officer, in particular of the following elements:

- the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred Personal Data; the economic sector in which the transfer occurs; the storage location of the data transferred;

- the laws and practices of the applicable local law - including those requiring the disclosure of data to public authorities or authorizing access by such authorities - relevant in light of the specific circumstances of the transfer, the applicable limitations and safeguards, and the enforceability of data subject rights and the effectiveness of legal remedies for data subjects;

- any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under the Processor Policy and as instructed by the Controller, including measures applied during transmission and to the processing of the Personal Data in Sodexo entities.

Sodexo entities agree to document this assessment and make it available to the Controller and to competent supervisory authority on request.

Where a Sodexo entity has reason to believe that the applicable local law and/or practices or a disclosure request may prevent it from fulfilling its obligations under the Processor Policy or its contractual obligations with the Controller and has a substantial effect on its ability to comply with this Processor Policy or its contractual obligations with the Controller, it promptly informs, in accordance with the service agreement, contract or any other binding document concluded with the Controller (a Client):

- the Sodexo entity acting as Data Exporter, that shall forward the notification to the Controller, who is entitled to suspend the transfer of Personal Data and/or terminate the contract or other binding document with Sodexo; and,

- Sodexo SA or,

- the Group Data Protection Officer and any other relevant Local Single Data Protection Points of Contact.

Following this notification, Sodexo SA together with the Sodexo entity acting as Data Exporter shall promptly, with the assistance of the Group Data Protection Officer, and if necessary, the relevant Local Single Data Protection Point of Contact, and if appropriate in consultation with the Controller, identify appropriate measures (e.g., technical or organizational measures to ensure security and confidentiality) to be adopted to address the situation.

Sodexo shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the Controller or the competent Supervisory Authority to do so. In this case, the Sodexo entity located outside of the EU/EEA which believes that it is or

has become subject to laws or practices not in line with the requirements of the Processor Policy shall not be a part of the BCR-Processor.

Request for Disclosure of the Personal Data by a law enforcement authority or state security body

In case of legally binding request for disclosure of the Personal Data or any direct access to Personal Data by a law enforcement authority or state security body, the Sodexo entities receiving it or becoming aware of it, will promptly notify Sodexo SA, the Group Data Protection Officer, and the Sodexo entity acting as Data Exporter.

The Sodexo entity acting as Data Exporter shall forward the notification to the Controller, and where possible, the data subject if instructed by the Controller.

Sodexo assesses each data access request by any law enforcement authority or state security body on a case-by-case basis. Sodexo uses its best efforts to inform the requesting authority concerned about Sodexo's obligations under the GDPR and to obtain the right to waive this prohibition.

Sodexo puts such request on hold for a reasonable delay in order to notify the above-mentioned stakeholders for this Processor Policy prior to disclosing the data to the requesting authority. Sodexo clearly informs the above-mentioned stakeholders about the request, including, but not limited to, information about the data requested, the number of requests, the requesting authority concerned, and the legal basis for the disclosure.

If in specific cases the suspension and/or notification are prohibited, Sodexo uses its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible and be able to demonstrate it, by documenting the best efforts taken.
If, despite having used its best efforts, Sodexo is not in a position to notify the above-mentioned stakeholders and to put the request on hold, in such case Sodexo provides general information about the requests it has received to the above-mentioned stakeholders (e.g. number of applications for disclosure, type of data requested, requesting authority if possible), to the extent it has been authorized by the said requesting authority to disclose such information to third parties. The Sodexo entity acting as Data Exporter shall forward this information to the Controller.

In any case, that transfers of Personal Data to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

Cross-border data transfers or disclosures not authorized by Union law

For Sodexo entities located in the EEA, any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a Controller or Processor to transfer or disclose Personal Data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to Chapter V of GDPR.

Any Sodexo entity receiving such request will promptly informs, in accordance with the service agreement, contract or any other binding document concluded with the Controller (a Client):

- the Sodexo entity acting as Data Exporter, that shall forward the notification to the Controller, who is entitled to suspend the transfer of Personal Data and/or terminate the contract or other binding document with Sodexo; and,
- Sodexo SA or,
- the Group Data Protection Officer and any other relevant Local Single Data Protection Points of Contact.

RULE 24 - COOPERATION WITH SUPERVISORY AUTHORITIES

RULE 24 - Sodexo assists the Controller in the fulfilment of its obligation of cooperation with Supervisory authorities and in accordance with the BCR Cooperation Procedure.

Under the Processor Policy, Sodexo entities assist the Controller in the fulfilment of its obligation of cooperation with Supervisory Authorities and in accordance with the BCR Cooperation Procedure in Appendix 3 and, in particular, cooperate with, and accept to be audited by the Supervisory Authorities and to comply with the advice of these Supervisory Authorities competent on any issue related to those BCR.

RULE 25 - BCR UPDATE

RULE 25 - Sodexo complies with the BCR Updating Procedure.

According to the BCR Updating Procedure in Appendix 4, Sodexo reports once a year any administrative changes to the Processor Policy or to the list of Sodexo entities adhering to the BCR to the relevant Supervisory Authorities, via the competent Supervisory Authority (i.e., the CNIL), with a brief explanation of the reasons justifying the update.

In case of any material changes that would possibly affect the level of protection offered by the BCR or significantly affect the BCR (i.e., changes to the binding character), it is communicated promptly to the relevant Supervisory Authorities, via the competent Supervisory Authority (i.e., the CNIL).

Any change to the BCR is notified to employees through Sodexo's intranet and to other Data Subjects and Controllers on Sodexo's official website.

In case of any material changes to the BCR, Sodexo also informs the Controller of any change that may affect the processing activities as agreed contractually. The Controller has the possibility to object to such a change or to terminate the service agreement, contract or any other binding document. The Group Data Protection Officer keeps a fully updated list of the Sodexo entities members of the BCR, with the support of the Group Legal team, and keeps track of and records any updates to the BCR and provides the necessary information to the Controller.

Sodexo ensures that no transfer is made to a new Sodexo entity as long as this entity is not effectively bound by the BCR or any other appropriate safeguards and cannot deliver compliance.

RULE 26 - BCR BINDINGNESS

RULE 26 - All Sodexo entities as part of the Sodexo Group acting as a Processor comply with the Processor Policy, including their employees.

When acting as Processor, Sodexo entities which have adhered to the Processor Policy, provide the Processor Policy to the Controller as part of the service agreement, contract or any other binding document with the Controller.

When Sodexo entities as a Processor subcontract their obligations with the prior consent of the Controller, they do so only by way of a written agreement with the subprocessor.

Where a non-EEA BCR member ceases to be part of the Sodexo Group or to be bound by the BCR, such Sodexo entity continues to apply the BCR requirements to the processing of those Personal Data transferred to it by means of the BCR, unless, at the time of leaving the Sodexo Group or ceasing to be bound by the BCR, that member deletes, anonymises or returns the entire amount of these Personal Data to a Sodexo entity to which the BCR still apply.

The Processor Policy has been shared with all employees as a new Group Data protection policy and is available at any time on the official Sodexo's intranet and official website.

All Sodexo employees are compelled to ensure confidentiality and comply with the data protection policies as set out in the data protection clause included in their employment contract. Appropriate disciplinary sanctions or judicial action in accordance with the law can apply in case of non-compliance with such data protection policies.

04

Appendices

- Appendix 1: Definitions
- Appendix 2: Global Data Collection and Data Retention Policy (Processor)
- Appendix 3: BCR Cooperation Procedure
- Appendix 4: BCR Updating Procedure
- Appendix 5: Sodexo Global Data Protection Policy
- Appendix 6: Global Data Protection Rights Management Policy
- Appendix 7: Description of the material scope of the Processor Policy

Appendix 1 - Definitions

When the subject matter herein concerns Personal Data, the non-capitalized terms and expressions used, e.g., “Personal Data”, “processing” etc., will be construed in accordance with the meaning given to them in the GDPR. In addition, the capitalized terms set out herein will for the purpose of these BCR have the meanings assigned to them below.

- **Adequate Country** means a country that ensures an adequate level of protection according to an “adequacy decision” adopted by the European Commission, the latter having the power to determine whether a third country ensures an adequate level of protection for Personal Data by reason of its domestic law or the international commitments it has entered into with.

- **Client** means external organizations or corporations establish in the EU or the EEA, that ask the Sodexo Group to perform services on their behalf for their employees / On-site personnel that are the end-users of these services, being the Controller.

- **Controller** means the entity that determines the purposes and means of the Personal Data processing.

- **Data Exporter** means a Controller (or, where permitted, a Processor) established in the EU that transfers Personal Data to a Data Importer.

- **Data Importer** means a Controller or Processor located in a third country that receives Personal Data from the Data Exporter.

- **Data Subject** means an identified or identifiable individual whose Personal Data is concerned by processing within the Sodexo Group, including the Personal Data of Sodexo’s current, past and prospective applicants, employees, clients, consumers/beneficiaries, suppliers/vendors, contractors/subcontractors, or any third parties.

- **EDPB** means the European Data Protection Board. It is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between the EU’s data protection authorities.

- **EU** means the European Union.

- **EEA** means the European Economic Area.

- **General Data Protection Regulation or GDPR** means 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.

- **Group Data Protection Officer** means the person appointed with Sodexo Group Executive Committee endorsement to oversee data privacy issues at the Sodexo Group level to define and spread Sodexo data protection compliance program and good practices relating to data privacy and to ensure their implementation as set out in Rule 20.

- **Local Single Data Protection Point of Contact** means the individual appointed by a Sodexo entity, in charge of handling local data privacy issues. In some cases, the Local Single Data Protection Point of Contact can be appointed as Local Data Protection Officer where required by applicable data protection law.

- **Personal Data** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Personal Data Breach** means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

- **Processing or Personal Data Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **Processor** means the individual or legal entity, agency or any other body who processes Personal Data on behalf of the Controller.

- **Sensitive Personal Data** designated as “Special Categories of Data” under the GDPR means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union memberships and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. This definition includes also Personal Data relating to criminal convictions and offences.

- **Sodexo Global Data Protection Program** means the program presented and validated by the Group Data Protection Officer to the Sodexo Group Executive Committee.

- **Sodexo Group or Sodexo entity or Sodexo entities or Processor Policy members** means any company or economic interest which is directly or indirectly owned by Sodexo with at least 50% of the share capital and voting rights and which is bound with the Sodexo Binding Corporate Rules.

- **Supervisory Authority** means an independent public authority which is established by a Member State as specified in the GDPR.

Appendix 2 - Global Data Collection and Data Retention Policy (Processor)

PREAMBLE

Sodexo is committed to protecting the privacy of its employees, clients, consumers and any other individuals and has implemented robust privacy policies, programs and practices. In particular, when Sodexo, being a Processor, carries out Personal Data Processing under the documented instructions of a Controller.

In order to meet best practices on Personal Data retention, Sodexo has adopted a Global Data Retention Policy. The present Policy describes how Sodexo, when it acts as a Processor, follows the principles of the GDPR and any other applicable laws and therefore how Sodexo ensures the protection of the rights and freedoms of the individuals.

DEFINITIONS

- **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. In this policy, Controller means a Client.

- **Data subject** means an identified or identifiable individual whose Personal Data is concerned by processing within the Sodexo, including the Personal Data of Sodexo's current, past and prospective applicants, employees, clients, consumers/beneficiaries, suppliers/vendors, contractors/subcontractors, or any third parties.

- **General Data Protection Regulation or GDPR** means 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.

- **Personal Data** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Personal Data Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **Sodexo entity or Sodexo entities** means any corporation, partnership or other entity or organization which is admitted from time to time as member of the Sodexo Group.

HOW TO ASSIST THE CONTROLLER IN COMPLYING WITH ITS STORAGE LIMITATION REQUIREMENT

a. Complying with the instruction of the Controller regarding Personal Data retention period

The Processor always needs to comply with the instructions of the Controller during the Personal Data Processing. This also applies to the deletion of the Personal Data at the end of the life cycle of the Processing.

Personal Data will therefore always be kept and/or deleted and/or anonymized under the instructions of the Controller in compliance with the Personal Data retention period set out by it, provided that such instructions do not conflict with applicable local laws.

Therefore, if during the performance of the contract, the Controller further instructs Sodexo to delete or return some of the Personal Data processed, Sodexo will have to comply with this instruction (provided that such instruction does not conflict with applicable local laws).

Sodexo will dispose of Personal Data only in a secure manner in accordance with the Group Information & Security Policy

b. Termination of the contract

Sodexo and its sub-processors (if any) will request the Controller to determine its choice with regards to the deletion or return or anonymization of the Personal Data. The choice will be specified in the contract or other binding document with that Controller.

On termination of the provision of the services relating to the Personal Data Processing, Sodexo as Processor and its sub-processors (if any), will act in accordance with the choice of the Controller expressed in the contract and delete, anonymize or return all the Personal Data transferred and the copies thereof to the Controller and will demonstrate that it has done so by providing an attestation to the Controller. This attestation should include at least the date of the deletion or anonymization, the list of Personal Data deleted or anonymized and the signature of the business owner concerned and the Data Protection Officer or the Local Single Data Protection Point of Contact. If applicable local laws set out a mandatory data retention period of the Personal Data and requires Sodexo to retain the Personal Data accordingly, Sodexo warrants that it will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore except for the purpose for which it is legally retained.

If the Controller has not contractually expressed its choice, Sodexo shall request the Controller to communicate its decision regarding the Personal Data at the termination date of the contract, at the latest.

Finally, Sodexo acting as Processor will inform each Sodexo entity to whom the Personal Data has been sub-processed of any deletion or anonymization of data and will require from each Sodexo entity aforementioned to do the same.

Appendix 3 - BCR Cooperation Procedure

1. This Cooperation Procedure sets out the way in which Sodexo entities adhering to the BCR shall cooperate with their competent Supervisory Authorities on any request or issue related to the implementation, the interpretation or the application of the BCR.

2. Sodexo entities adhering to the BCR shall make the necessary personnel available for dialogue with the competent Supervisory Authorities.

3. Sodexo entities adhering to the BCR shall comply with any decisions or advice made by the competent Supervisory Authorities on any data protection law issues that may affect the implementation, the interpretation or the application of the BCR.

4. Sodexo entities adhering to the BCR shall actively review and consider the guidelines, recommendations and best practices issued or endorsed by the European Data Protection Board that may affect the implementation, the interpretation or the application of the BCR.

5. Sodexo entities adhering to the BCR agree to abide by a formal decision from the competent Supervisory Authorities, on any issues related to the implementation, the interpretation or the application of the BCR.

6. Sodexo entities adhering to the BCR shall communicate without undue delay to the competent Supervisory Authorities any material changes to the BCR in accordance with the Updating Procedure (Appendix 4 of the BCR).

7. Sodexo entities adhering to the BCR shall answer to any request for information or complaint from the competent Supervisory Authorities.

8. Upon request, Sodexo entities adhering to the BCR shall provide the competent Supervisory Authorities with a copy of the results of any assessment of compliance with the BCR and/or other documentation requested, and the ability to conduct an audit of Sodexo entities adhering to the BCR for the purpose of reviewing compliance with the BCR.

Appendix 4 - BCR Updating Procedure

Preamble

1. This Updating Procedure sets out the way in which Sodexo shall communicate changes to the BCR to the competent Supervisory Authorities, the Clients, the Data subjects and to the Sodexo entities adhering to the BCR.

Material changes

2. Sodexo will communicate promptly any material changes to the BCR (understood as any changes that would possibly affect the level of the protection offered by the BCR or which would significantly affect the BCR, such as changes to the binding character of the BCR) to the relevant Supervisory Authorities, via the Commission Nationale de l'Informatique et des Libertés ("CNIL"), acting as Sodexo's lead Supervisory Authority.

3. Where a material change to the BCR affects the conditions under which Sodexo processes Personal Data on behalf of a Client under the terms of a contract or other binding document that Sodexo has signed with that Client, Sodexo shall:

    a. Communicate the proposed change before implementing it, and with sufficient notice to enable the affected Client to object; and

    b. Allow the Client to suspend the transfer of Personal Data to Sodexo and/or terminate its relationship with Sodexo, in accordance with the terms of its contract or other binding document with Sodexo.

Administrative changes

4. Sodexo will communicate changes to the BCR which are administrative in nature (including changes in the list of Sodexo entities adhering to the BCR) to the relevant Supervisory Authorities, via the CNIL at least once a year. Sodexo will also provide a brief explanation of the reasons for any communicated administrative changes to the BCR.

Communication to Data Subjects and Sodexo entities adhering to the BCR

5. Sodexo shall communicate without undue delay all changes to the BCR, whether administrative or material in nature, to the Sodexo entities adhering to the BCR and to the Clients.

6. Sodexo shall communicate administrative or material changes to the Data subjects who benefit from the BCR via Sodexo's intranet and official website.

Role of the Group Data Protection Officer

7. The Group Data Protection Officer, with the support of the Global Data Protection Office, will (i) keep a fully updated list of Sodexo entities adhering to the BCR and of the sub-

processors involved in the data processing activities for the Clients (acting as controller); (ii) make accessible to the Clients (acting as controller), the Data Subjects and the Supervisory Authorities the above-mentioned fully updated list; and (iii) keep track of and record any updates to the BCR and provide the necessary information systematically to the Clients (acting as controller) and/or Supervisory Authorities upon request.

8. Sodexo shall ensure that no transfer is made to a new Sodexo entity as long as this entity is not effectively bound by the BCR or any other appropriate safeguards and cannot ensure compliance with the BCR.

Appendix 5 - Sodexo Global Data Protection Policy

Link to the Sodexo Global Data Protection Policy published on Sodexo SA corporate website.

Appendix 6 - Global Data Protection Rights Management Policy

Link to the Global Data Protection Rights Management Policy published on Sodexo SA corporate website.

Appendix 7 - Description of the material scope of the Processor Policy

Types of Personal Data Processing carried out and/or contemplated and purposes	Categories of Data Subjects concerned	Categories of Personal Data processed	List of countries of destination
▬ Performance of the services provided by Sodexo on behalf of Clients (e.g., Facilities Management services, food services, some of the Benefits & Rewards services[11]).	▬ Clients (current or potential business contacts) ▬ Consumers/Beneficiaries (current or potential consumers or beneficiaries)	▬ Identification data (civil status, identity…) ▬ Professional life ▬ Connection data (e.g., credentials for authentication purposes, logs/interaction with the relevant IT applications, IP address)	▬ All countries where Sodexo entities operate.

[11] Services provided by Sodexo on behalf of Clients:

- On-site services:
  - Food services: catering, cafeteria, special dining, retail food operations and vending machines;
  - Facilities Management services:
    - Soft Facilities Management services: cleaning, laundry, reception, help desk, security;
    - Hard Facilities Management: technical maintenance, electric maintenance, building maintenance.
- Benefits and Rewards services:
  - Employee Benefits: Sodexo develops Meal Pass or Gift Pass to attract and retain employees and improve organizational efficiency
  - Diversification: Sodexo offers simple and easy-to-access solutions to meet mobility challenges, as well as health and wellness, and incentive and recognition via unique platforms such as fuel cards, Mobility Pass travel booking and management of business expenses.

Depending on the local regulation, for these services the Sodexo entities can be considered as processors.

04 Appendices