Sodexo Binding Corporate Rules

Controller Policy

Table of Contents

In this document, “Sodexo” refers collectively to the Sodexo entities who have adhered to the Controller Policy of the Binding Corporate Rules (“BCR”) by signing an intra-group agreement (“Sodexo entity” or “Sodexo entities” or “Controller 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 Controller 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) 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 Controller 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 Controller 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 Controller 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 Controller 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 Controller Policy members when handling Personal Data, irrespective of the country in which they are located.

This policy addresses the Processing of all Personal Data of Sodexo's current, past and prospective job applicants, employees, clients, consumers/beneficiaries, suppliers/vendors, contractors/subcontractors, or any third parties or by a third-party on behalf of Sodexo.

The Controller Policy covers the processing of Personal Data by Sodexo entities established within Europe legally bound by the BCR 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.

The material scope of this Controller Policy is described in Appendix 8.

- 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 the EU/EEA by a Sodexo entity acting as a Controller, or transferred to a Sodexo entity outside the EU/EEA, acting as a Controller or as a Processor, have rights to complain or obtain judicial remedies and appropriate redress and, where appropriate, receive compensation for any breach of the rules contained in the Controller Policy (Data Protection principles, transparency on BCR and easy access, Data Subjects' rights, transparency on where the legislation prevents Sodexo Group from complying with the BCR, liability, right to complain and to obtain judicial remedies and cooperation duties with Supervisory Authorities) as third party beneficiaries as detailed in Rule 21 of the BCR.

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 Controller Policy and any other underlying policies and procedures.

Business owners 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 this Controller 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 Controller 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 Controller Policy are divided into two Sections:

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

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

Section A

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

RULE 1 - Sodexo complies first and foremost with the provisions of the Controller 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 Controller Policy, set out in accordance with the GDPR.

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 Controller Policy.

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

RULE 2 - ENSURING LAWFULNESS, FAIRNESS AND TRANSPARENCY

RULE 2 - Sodexo ensures lawfulness, fairness and transparency.

Lawfulness: all Personal Data are processed based on one or more of the following legal grounds:

(i) Sodexo is subject to a legal obligation to process Personal Data;

(ii) Processing is necessary for (i) the performance of a contract to which the Data Subject is a party or (ii) to take steps at the request of the Data Subject prior to entering into a contract;

(iii) Processing is necessary for the purposes of Sodexo or a third party's legitimate interest (for example harmonization, standardization and streamlining of professional roles and processes, engagement surveys among employees, management of workspace occupancy, optimization of workspaces, or enhancing of customer relationship management), except where such purposes are overridden by the fundamental rights and freedom of the Data Subjects;

(iv) Processing relies on Data Subject's free, unambiguous and specific consent.

Fairness and transparency: Sodexo provides all required information to the Data Subjects on the conditions of processing and on how to exercise their rights, notably in the Global Data Protection Policy in Appendix 2. The types of required information are detailed in Appendix 3 (Table on transparency).

RULE 3 - ENSURING PURPOSE LIMITATION

RULE 3 - Sodexo uses Personal Data for a known, relevant and legally grounded purpose only.

Personal Data is collected and processed by Sodexo for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

RULE 4 - ENSURING DATA MINIMIZATION

RULE 4 - Sodexo ensures that Personal Data processed is adequate, relevant and limited to what is necessary for the purposes for which it is originally collected and processed.

Sodexo ensures that Personal Data collected, processed and/or stored is adequate, relevant and limited to what is necessary for the purposes for which it is originally collected and processed.

RULE 5 - ENSURING ACCURACY

RULE 5 - Sodexo keeps Personal Data that is processed accurate and, where necessary, up to date.

When Personal Data is inaccurate, considering the purposes for which it is processed, Sodexo takes all reasonable steps to erase or rectify the Personal Data. In order to ensure that the Personal Data held by Sodexo remains accurate and up to date, Sodexo actively encourages Data Subjects to inform Sodexo of any changes and intends to develop user-friendly interfaces and tools allowing Data Subjects to directly update their Personal Data.

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

Sodexo, acting as a Controller, 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 keeps Personal Data for only as long as necessary.

Personal Data processed by Sodexo is kept in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed and in line with the Sodexo Global Data Collection and Data Retention Policy (Appendix 6) and the defined data retention periods.

However, Personal Data is stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or as required by applicable local law, for instance EU/EEA legislation.

Sodexo disposes of Personal Data only in a secure manner in accordance with the Sodexo Group Information & Systems Security Policy.

RULE 7 - TAKING APPROPRIATE TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

RULE 7.A - Sodexo processes Personal Data in compliance with the Sodexo Group Information & Systems Security Policy.

Personal Data is processed by Sodexo in compliance with the Group Information & Systems Security Policy as revised and updated from time to time, in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational security measures. Sodexo implements enhanced security measures to process Sensitive Personal Data.

Sodexo notifies security breaches to the Supervisory Authorities and/or to the Data Subjects as required by GDPR when it becomes aware of the Personal Data Breach in accordance with the Group Security Directive on Information Security Incident Management[4].

RULE 7.B - Sodexo ensures that any Processor, internal or external, acting on behalf of any Sodexo entity, being the Controller, adopts appropriate technical and organizational security measures.

When Sodexo acts as a Controller, it ensures that when it uses a Processor, internal or external, the said Processor provides sufficient written and documented commitments to process Personal Data in respect of the appropriate technical security measures and organizational measures governing the Processing to be carried out.

When Sodexo engages an internal Processor (i) Sodexo only uses either Sodexo entities based within the EU/EEA or in an Adequate Country or, Sodexo entities located outside of EU/EEA who have adhered to this Controller Policy; and (ii) the internal Processor commits to respect the obligations set forth in Article 28 of the GDPR.

If Sodexo uses external Processors, the Processing shall be governed by a contract or other legal act under Union or Member State law, that is binding on the Processor with regard to Sodexo and that sets out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of personal data and categories of data subjects and the obligations and rights of the Controller.

That contract or other legal act shall stipulate, in particular, that the Processor:

(i) Processes the Personal Data only on documented instructions from Sodexo, including with regard to transfers of Personal Data to a third country or an international organization,

4 Internal document

unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform Sodexo of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(ii) ensures that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(iii) takes all measures required pursuant to Article 32 of the GDPR;

(iv) respects the conditions referred to in paragraphs 2 and 4 of article 28 of the GDPR for engaging another Processor;

(v) taking into account the nature of the Processing, assists Sodexo by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Sodexo's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

(vi) assists Sodexo in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of Processing and the information available to the Processor;

(vii) at Sodexo's choice, deletes or returns all the Personal Data to Sodexo after the end of the provision of services relating to Processing, and deletes existing copies unless Union or Member State law requires storage of the Personal Data;

(viii) makes available to Sodexo all information necessary to demonstrate compliance with the obligations laid down in article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Sodexo or another auditor mandated by Sodexo.

The Processor shall immediately inform Sodexo if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

Without prejudice to an individual contract between Sodexo and the Processor, the contract or the other legal act referred to above may be based, in whole or in part, on standard contractual clauses of the European Commission, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43 of the GDPR.

RULE 7.C - Sodexo reports any Personal Data Breach to the relevant Supervisory Authority(ies) and/or the affected Data Subjects, if any, in accordance with the Group Security Directive on Information Security Incident Management.

In the event of a Personal Data breach, the breach is notified to Sodexo SA, as EU headquarters, and, in particular, to the Global Data Protection Office, and to the relevant Local Single Data Protection Points of contact.

This Personal Data breach is notified to the relevant Supervisory Authority(ies) without undue delay, and in any event within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of Data Subjects.

The Group Data Protection Officer and the Local Single Data Protection Points of Contact in their respective jurisdictions, keep documented records of all Personal Data Breaches, comprising the facts and effects of the breach and any remedial action taken. Such records shall be made available to the Supervisory Authorities on request.

In the event of a Personal Data Breach is likely to result in a high risk to the rights and freedoms of Data Subjects, the affected Data Subjects are notified without undue delay, unless Sodexo is exempted to do so according to the GDPR.

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

RULE 8 - Sodexo processes Sensitive Personal Data and other Special Categories of Personal Data only if it is strictly necessary to achieve the purpose of the Personal Data Processing and if there is a legal ground to do so.

Sodexo processes Sensitive Personal Data and other Special Categories of Personal Data if:

(i) the Data Subject has given explicit consent to the Processing;

(ii) Processing is necessary for the purposes of carrying out Sodexo's obligations and exercising its specific rights or of the Data Subject rights under employment and social security and social protection applicable local laws or a collective agreement pursuant to local law;

(iii) Processing is necessary to protect the vital interests of the Data Subject or of another individual where the Data Subject is physically or legally incapable of giving consent;

(iv) Processing relates to Personal Data which are manifestly made public by the Data Subject;

(v) Processing is necessary for the establishment, exercise or defence of legal claims;

(vi) Processing is necessary for reasons of substantial public interest, on the basis of applicable local law;

(vii) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of employees, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of applicable local law or pursuant to a contract with a healthcare professional;

(viii) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of applicable local law;

(ix) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

In such case, Sodexo limits access to Sensitive Personal Data and other Special Categories of Personal Data to appropriate persons and processes such data, in accordance with the Group Information & Systems Security Policy[5].

RULE 9 - KEEPING RECORDS OF DATA PROCESSING ACTIVITIES

RULE 9 - Sodexo keeps records of its Controller's processing activities.

Sodexo keeps records of its Controller's processing activities, in writing, in a dedicated accountability tool and in accordance with Article 30.1 of the GDPR.

Meaning that the records contain all the following information:

(i) the name and contact details of the Controller and, where applicable, the joint Controller, the Controller's representative and the data protection officer;

(ii) the purposes of the processing;

(iii) a description of the categories of data subjects and of the categories of Personal Data;

(iv) the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organizations;

(v) where applicable, transfers of Personal Data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, the documentation of suitable safeguards;

[5] Internal document.

(vi) where possible, the envisaged time limits for erasure of the different categories of data;

(vii) 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.

In addition, Sodexo complies with any additional applicable local requirements, that requires a higher level of protection for Personal Data, in terms of keeping records of data processing activities or filing requirements.

RULE 10 - HONOURING DATA SUBJECTS RIGHTS

RULE 10 - Sodexo honors Data Subjects' rights.

The Data Subjects are entitled to the following:

Right of access

The Data Subject has access to the Personal Data relating to him/her processed by Sodexo.

Right to rectification or erasure/right to be forgotten

The Data Subject has the right to obtain from Sodexo without undue delay the rectification of inaccurate Personal Data concerning him or her or the right to have incomplete Personal Data completed.

The Data Subject has the right to obtain from Sodexo the erasure of Personal Data concerning him or her without undue delay notably (i) when the Personal Data is no longer necessary in relation to the purposes for which they were collected, (ii) the Data Subject withdraws consent on

which the Processing is based, or and where there is no other legal ground for the processing, (iii) the Data Subject objects to the Processing, (iv) the Personal Data has been unlawfully processed, (v) the Personal Data has to be erased for compliance with a legal obligation under applicable local law, (vi) the Personal Data has been collected in relation to the offer of information society services[6] (e.g. e-commerce services, public websites).

Sodexo notifies the Data Subject when it cannot respond favorably to such right of erasure/right to be forgotten, if the Personal Data is necessary (i) for exercising the right of freedom of expression and information, (ii) for compliance with a legal obligation, (iii) for reasons of public interest in the area of public health, (iv) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, (v) for the establishment, exercise or defense of legal claims.

Right to object

The Data Subject has the right to object, at any time, to the processing of Personal Data concerning him or her which is used for marketing purposes or leads Sodexo to take decision based solely on automated processing, including profiling, which produces legal effects concerning a Data Subject or similarly significantly affects him or her, and based on the following grounds:

- the performance of a task carried out in the public interest or in the exercise of official authority vested in Sodexo;

- the purposes of the legitimate interests pursued by Sodexo or by a third party.

If the Data Subject exercises such right to object, Sodexo no longer processes the Personal Data unless Sodexo demonstrates compelling legitimate grounds for the processing or for the establishment, exercise or defense of legal claims.

However, if the Data Subject objects to Processing for direct marketing purposes, the Personal Data is no longer processed for such purposes.

Right to restriction

The Data Subject has the right to obtain from Sodexo restriction of processing where (i) the accuracy of the Personal Data is contested by the Data Subject, for a period enabling Sodexo to verify the accuracy of the Personal Data, (ii) the Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests instead restriction of their use, (iii) Sodexo no longer needs the Personal Data for the purposes of the processing, but the Data Subject requires them for the establishment, exercise or defense of legal claims, (iv) the Data Subject has objected to processing, restriction applies pending the verification whether the legitimate grounds of Sodexo override those of the Data Subject.

[6] Under the Article 1(2) of Directive 98/34/EC, « information society services » means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of the GDPR, “information society services” means a service as defined in point (b) of Article 1 (1) of the Directive (EU) 2015/1535 of the European Parliament and of the Council essentially, any services requested and delivered over the internet, “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services”.

The Data Subject who has obtained restriction of Processing is informed by Sodexo before the restriction of Processing is lifted.

Right to portability

The Data Subject has the right to receive the Personal Data concerning him or her, which he or she has provided to Sodexo, in a structured, commonly used and machine-readable format and has the right to transmit those data to another service provider or third party.

Such right to portability applies, subject to the rights and freedoms of others, in the following cases:

- the Processing is based on consent or a contract; and
- the processing is carried out by automated means.

Data Subjects are informed about their rights and how they can exercise their rights in the Global Data Protection Rights Management Policy, as set out in Appendix 7.

Sodexo responds to the Data Subjects concerned within a reasonable timeframe and in compliance with the required response time under the GDPR or any other applicable local law, that has a stricter required response time.

Right to lodge a complaint

The Data Subject has the right to lodge a complaint in accordance with Rule 17 of the BCR with the Supervisory Authority in the country of his or her habitual residence, place of work or place of the alleged infringement, regardless of whether the person has suffered damages. Also, the Data Subject has the right to lodge a claim with the court where Sodexo has an establishment or where the person has his or her habitual residence.

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

RULE 11 - Sodexo does not conduct any evaluation or take any decision about the Data Subjects which may significantly affect them or produce legal effects concerning them and based solely on automated processing of their Personal Data, including profiling, unless in certain limited cases and with suitable safeguards having been implemented.

Sodexo does not conduct any evaluation or take any decision about the Data Subjects which may significantly affect them or produce legal effects concerning them based solely on automated processing of their Personal Data, including profiling, unless in the following cases, notably when it is:

- necessary for entering into, or performance of, a contract between the Data Subject and Sodexo;
- authorized by the applicable local law to which Sodexo is subject and which provides suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests, especially if this local law requires a higher level of protection for Personal Data; or
- is based on the Data Subject's explicit consent.

In such case, Sodexo implements suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests, which should include at least the right to obtain human intervention on the part of the Controller, to express his or her point of view and to contest the decision and any other safeguards required by applicable local law.

Sodexo does not conduct automated decision or profiling activities on special categories of data unless suitable safeguards are in place to protect the Data Subject’s rights and legitimate interests.

Sodexo clearly informs the Data Subject on the conditions of such automated Personal Data Processing and the safeguards implemented to protect Data Subject’s rights and legitimate interest.

In addition, Sodexo does not implement such automated Personal Data Processing, including Profiling without conducting a Data Protection Impact Assessment as described in Rule 15 of this Controller Policy.

RULE 12 - TRANSPARENCY AND DATA SUBJECT'S INFORMATION

RULE 12.A - Sodexo makes the Controller Policy readily available to the Data Subjects.

Sodexo makes the Controller Policy available to the Data Subjects by publishing it on its official website. In addition, the Global Data Protection Policy (Appendix 2) includes a dedicated schedule on the third-party beneficiary rights.

RULE 12.B - Sodexo commits to provide Data Subjects with comprehensive information notices and Data protection policies as appropriate prior to collection and process their Personal Data in compliance with GDPR and any other applicable local law that would require a higher level of protection for Personal Data, for instance EU legislation.

Sodexo commits to provide Data Subjects with comprehensive information notices and Data protection policies, such as the Global Data Protection Policy (in Appendix 2), in compliance with the Table on transparency (Appendix 3) or, where applicable, through a layered approach as appropriate prior to collection and process their Personal Data in compliance with GDPR and any applicable local law that requires a higher level of protection for Personal Data, for instance EU legislation.

All Data Subjects benefiting from the third-party beneficiary rights in particular are provided with the information required by the GDPR in full, on their third-party beneficiary rights with regard to the Processing of their Personal Data and on the means to exercise those rights, the clause relating to the liability and the clauses to the Data Protection principles.

RULE 13 - ENSURING ADEQUATE PROTECTION FOR CROSS-BORDER 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.

Cross-border data transfers to third parties outside the Sodexo Group (or to a Sodexo entity that is not bound by this Controller Policy) located outside the EU/EEA or in a country which has not been recognized by the European Commission as an Adequate Country are not allowed without taking adequate safeguards, such as the signature of a data transfer agreement based on the European Commission standard contractual clauses, and, if applicable, the implementation of supplementary measures as needed in accordance with Schrems II ruling[7], and applicable EDPB guidelines, that may be amended from time to time.

[7] Decision C-311/18 - Facebook Ireland and Schrems of the European Court of Justice of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems

RULE 14 - EMBRACING PRIVACY BY DESIGN AND BY DEFAULT

RULE 14 - Sodexo embraces privacy by design for every new digital project or new business opportunity involving Personal Data Processing and privacy by default by training its personnel handling Personal Data and implementing procedures to ensure that each time Personal Data is processed, appropriate technical and organizational measures are put in place.

Privacy by design

Where a new digital project or a new business opportunity is initiated, involving Personal Data Processing, data protection is taken into account, both at the time of the definition of the means and the related appropriate technical and organizational security measures for the Personal Data Processing and at the time of the implementation of Processing itself. The same principle applies where Sodexo intends to merge with or acquire a company, it makes sure that data protection principles are respected.

Sodexo has developed an end2end privacy compliance process, including a Data Protection Risk Assessment process for use by business owners, IT applications owners and project managers involved in the above-mentioned projects.

Privacy by default

Sodexo trains its personnel handling Personal Data and implements procedures to ensure that each time Personal Data is processed, appropriate technical and organizational measures are taken for ensuring that, by default, only Personal Data which is necessary for each specific purpose is processed (in terms of amount of data processed, extent of the processing and data retention) and is made accessible only to a limited number of persons who need to know.

RULE 15 - CONDUCTING DATA PROTECTION IMPACT ASSESSMENT (DPIA)

RULE 15 - Sodexo conducts a Data Protection Impact Assessment (DPIA) where it is required.

For all projects involving Processing of Personal Data, an end-to-end Data Protection Risk Assessment process is completed to check compliance with data protection principles, to assess impact on Data Subjects' rights and to check implementation of privacy by design & by default.

This process includes a Privacy Risk Assessment Questionnaire (the “PRAQ”) aimed at collecting all the information required to perform a risk analysis of the project/process under the applicable Data protection regulation and to check whether a full Data Protection Impact Assessment (‘DPIA’) is required in accordance with the end2end privacy compliance process. This process also permits to determine whether a new record of data processing activity should be created in the Sodexo’s GDPR Accountability tool or if an update of existing records should be done.

In accordance with the end2end privacy compliance process and the Article 35(3) of the GDPR, a DPIA will be required in the case of:

(i) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(ii) processing on a large scale of special categories of data referred to in Article 9(1) of the GDPR, or of Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or

(iii) a systematic monitoring of a publicly accessible area on a large scale.

When conducting a DPIA, the Global Data Protection Office and/or relevant Local Single Data Protection Points of Contact involves the relevant internal stakeholders.

A DPIA begins early in the life of a project but can run alongside the project implementation process. Where a DPIA indicates that the Personal Data Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risks, the competent Supervisory Authority, prior to processing, is consulted.

Section B

RULE 16 - TRAINING AND AWARENESS

RULE 16 - Sodexo provides appropriate training to employees who have permanent or regular access to Personal Data, who are involved in the collection of Personal Data or in the development of tools used to process Personal Data.

A comprehensive training program

To make the Controller 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 these BCR.

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.

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 provide training in compliance with local laws 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 this Controller Policy.

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

RULE 17 - DATA PROTECTION RIGHTS HANDLING

RULE 17 - Sodexo answers to requests, queries and concerns from Data Subjects and questions from the Supervisory Authorities following a complaint from Data Subjects.

Sodexo entities implement a local requests and complaints handling system in compliance with the Global Data Protection Rights Management Procedure[8].

The Local Single Data Protection Point of Contact responds to Data Subjects' requests without undue delay and, in any event, at the latest within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. Sodexo informs the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay. The Data Subjects are informed about: (i) how to exercise their rights and what steps to follow are; (ii) in which form; (iii) the timescale for the reply on the request; (iv) consequences in case of rejection of the request ; (v) consequences in case the request is considered as justified; (vi) if they believe that their data protection rights may have been breached, they have the right to lodge a complaint with the Supervisory Authority in the country of its habitual residence, place of work or place of the alleged infringement, regardless of whether the person has suffered damages and with the court where Sodexo has an establishment or where the person has its habitual residence, in accordance with the Global Data Protection Policy, including the Global Data Protection Rights Management Policy set out in Appendix 7, and/or the local data protection policies, available on the official Sodexo's websites.

Where the Sodexo entity has reasonable doubts concerning the identity of the Data Subject making the request, the Sodexo entity may request the provision of additional information necessary to confirm the identity of the Data Subject. If needed, the Local Single Data Protection Points of Contact advises the Data Subjects about practical steps of their local requests and complaints handling system.

If Local Single Data Protection Point of Contact receives a data protection related query or concern or questions from a Data Protection Supervisory Authority following a complaint, it is his/her role, in accordance with the Global Data Protection Rights Management Procedure[9], to explain, with the support of the relevant business/function owner which is accountable for the data processing activities at stake, to the Data Subjects or to the Data Protection Supervisory Authority in as much detail as we can how we have complied with the law, that we have done all we can to find an appropriate resolution or if something has gone wrong, to outline the steps taken to put it right.

[8] Internal Document

[9] Internal Document

RULE 18 - ASSESSMENT OF COMPLIANCE: AUDIT PROGRAM

RULE 18 - Sodexo complies with the Sodexo's BCR Audit Program relying on the BCR Compliance Check List.

According to the Sodexo Global BCR Audit Program Sodexo audits the Sodexo Group's compliance with the Controller Policy and in particular:

- Implements an audit plan which covers all aspects of the Controller Policy including methods of ensuring that corrective actions will take place.
- Such audit is carried out annually by the Internal Control team.
- Such audit is also carried out 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 Point(s) of Contact and to the 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 shall allow 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.

RULE 19 - MONITORING OF BCR APPLICATION

RULE 19 - Sodexo monitors the Controller Policy application.

To ensure the Controller 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 Controller Policy as well as Data Protection Impact Assessments carried out locally to the Global Data Protection Office on a 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 quarterly 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 Controller Policy through a Data Protection Governance Structure.

To oversee and ensure compliance with the Controller Policy, Sodexo has implemented 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 monitors compliance at a global level and assesses 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 reports to the highest management level and enjoys their support for the fulfilling of this task. The Group Data Protection Officer provides them with advice and recommendations regarding Sodexo acting as Controller as well as with a quarterly report of the Global Data Protection Office's activities. In addition, the Group Data Protection Office monitors 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 SPOC when needed to comply with the Sodexo Global Data protection Program, deals with Supervisory Authorities' investigations, and ensures that the Local DP SPOC handles local complaints from Data Subjects, reports major Data protection issues to the Group Data Protection Officer, ensures compliance at a local level and is being accessible, in local language, to the local Data Subjects and to the local Supervisory Authority, under the accountability of local business/function owner.

RULE 21 - THIRD-PARTY BENEFICIARY RIGHTS

RULE 21 - Sodexo confers expressly rights on Data Subjects to enforce the Controller Policy.

Data Subjects are able to enforce the following elements of the Controller Policy against the Sodexo entities:

- **Data protection principles**: Data Subjects may enforce Rules 2 (lawfulness, fairness and transparency), 3 (purpose limitation), 4 (data minimization), 5 (data accuracy), 6 (storage limitation), 8 (sensitive Personal Data and other special categories of data), 14 (privacy by design and by default), and 15 (data protection impact assessment) of the Controller Policy.

- **Transparency on the Controller Policy**: Data Subjects have easy access to their third-party beneficiary rights since the BCR are made available on Sodexo's intranet and official website. They may obtain a copy of this Controller Policy from the BCR members acting as Controllers upon request. In addition, the Global Data Protection Policy (Appendix 2) will include a dedicated schedule on the third-party beneficiary rights.

- **Data Subjects' rights**: Data Subjects may enforce Rule 10 by lodging a complaint in accordance with the Global Data Protection Rights Management Policy, as attached to the Sodexo Global Data Protection Policy (i) with the competent Supervisory Authority against the Sodexo entity responsible for exporting the data and acting as a Controller either before (a) 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 competent courts of the EU/EEA Member States (choice for the Data Subjects to act before the courts where the Controller has an establishment or where they have their residence).

- **Right to Complain**: Data Subjects may complain to a Local Single Data Protection Point of Contact in accordance with Rule 17 and the Global Data Protection Rights Management Policy set out in Appendix 7 which is also available in the Global Data Protection Policy. 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) and the right to lodge a claim before the Court or relevant Supervisory authority.

- **Liability**: Sodexo acting as Controller or Joint Controller will accept responsibility for and agrees to take the necessary actions to remedy the acts of other Sodexo entities established outside EU/EEA bound by the Controller Policy and to pay compensation for any damages resulting from a violation of the policy. If a Sodexo entity outside the EU/EEA violates the policy, the courts or competent authorities in France will have jurisdiction and the Data Subject will have the rights and remedies against Sodexo SA that has accepted responsibility and liability as if the violation had been caused by itself in France instead of the Sodexo entity concerned outside the EU/EEA. Data Subjects may lodge a complaint (a) with the French

Supervisory Authority (the "Commission Nationale de l'Informatique et des Libertés", the "CNIL") against Sodexo SA responsible for exporting the data, (b) with the Supervisory authority in the Member State of their habitual residence, (c) place of work or (d) 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. 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.

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

- **Compensation**: Data Subjects have right to judicial remedies and to obtain appropriate redress and, where appropriate, receive compensation in case of any breach of one of the abovementioned enforceable elements of the Controller Policy before the competent courts of the EU/EEA Member States (choice for the Data Subjects to act before the courts where the Controller has an establishment or where they have their residence).

- **Transparency where national legislation and practices prevents the group from complying with the BCR**: Data Subjects may enforce Rule 23.

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 Controller Policy, Sodexo SA, acting as Controller or Joint Controller, accepts responsibility for and agrees to take the necessary actions to remedy the acts of other Sodexo entities established outside EU/EEA bound by the Controller Policy and to pay compensation for any material or non-material damages resulting from a violation of the policy.

If a Sodexo entity outside the EU/EEA violates the BCR, the courts or other competent authorities in the EU have jurisdiction and the Data Subject have the rights and remedies against Sodexo SA that has accepted responsibility and liability as if the violation had been caused by Sodexo SA in the Member State in which they are based instead of the Sodexo entity concerned outside the EU/EEA.

Sodexo SA who has accepted liability 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 CONTROLLER POLICY - 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 Controller Policy and have not a substantial effect on its ability to comply with this Policy, especially to ensure that enforceable data subject rights and effective legal remedies for data subjects are available.

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

RULE 23.C - Sodexo ensures that where it receives a legally binding request for disclosure of Personal Data which is subject to the Controller Policy, it notifies Sodexo SA, Sodexo Group Data Protection Officer, the Sodexo entity acting as Data Exporter, and, where possible, the data subject, unless prohibited from doing so by a law enforcement authority. This 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[10] and the European Union Standard Contractual Clauses[11]:

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 Controller Policy and have a substantial effect on their ability to comply with this policy. 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 Controller Policy.

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:

[10] 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.

[11] 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.

- 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 appropriate 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 Controller Policy, 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 competent supervisory authority on request.

In addition, if any Sodexo entity located outside of the EU/EEA has reason to believe that it is or has become subject to laws and/or practices not in line with the requirements of the Controller Policy, it will promptly notify Sodexo SA, the Group Data Protection Officer, any other relevant Local Single Data Protection Point of Contact, in particular the Local Single Data Protection Point of Contact of the Sodexo entity acting as Data Exporter, and the Sodexo entity acting as Data Exporter.

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, identify appropriate measures (e.g., technical or organizational measures to ensure security and confidentiality) to be adopted to address the situation.

The Sodexo entity acting as Data Exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent Supervisory Authority to do so. In this case, the Sodexo entity located outside of the EU/EEA which believe that it is or has become subject to laws and/or practices not in line with the requirements of the Controller Policy shall not be a part of the BCR-Controller.

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, the Sodexo entity acting as Data Exporter, and, where possible, the data subject (if necessary, with the help of the Sodexo entity acting as Data Exporter).

The above-mentioned stakeholders are clearly informed about the request, including, but not limited to, information about the data requested, the number of requests, the requesting body and the legal basis for the disclosure (unless otherwise prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

In the specific cases in which the suspension and/or notification are prohibited, Sodexo entities use their best efforts to obtain the right to waive this prohibition in order to communicate as much information as they can and as soon as possible and be able to demonstrate that they did so by documenting the best efforts taken. If despite having used its best efforts, the requested Sodexo entities are not in a position to notify the relevant stakeholders, they provide them with general information on the requests received on an annual basis.

Sodexo entities agree to preserve the information regarding the request for disclosure of the Personal Data or any direct access to Personal Data by a law enforcement authority or state security body, and the best efforts they have taken to inform the above-mentioned stakeholders as described above.

Sodexo entities do not proceed to massive, disproportionate, and indiscriminate transfers of Personal Data to any public authority 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.

RULE 24 - COOPERATION WITH SUPERVISORY AUTHORITIES

RULE 24 - Sodexo complies with the BCR Cooperation Procedure.

Under the Controller Policy, Sodexo entities adhering to the BCR comply with the BCR Cooperation Procedure in Appendix 4 and, in particular, cooperate with, accept to be audited by the Supervisory Authorities and to comply with the advice of these Supervisory Authorities on any issue related to this policy.

RULE 25 - BCR UPDATE

RULE 25 - Sodexo complies with the BCR Updating Procedure.

According to the BCR Updating Procedure in Appendix 5, Sodexo reports promptly material changes to all Sodexo entities adhering to the BCR and to the relevant Supervisory Authorities, via the competent Supervisory Authority (i.e., the French Supervisory Authority, the CNIL).

In addition, updates to the BCR or to the list of the Sodexo entities adhering to the BCR are kept track of and recorded by the Group Data Protection Officer, with the support of the Group Legal team, who will provide the necessary information to the Data Subjects (via Sodexo's intranet and to third parties on Sodexo's official website). Sodexo reports once a year any administrative changes to the Controller 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.

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.

Any changes to the BCR or to the list of Sodexo entities adhering to BCR is reported annually to the relevant Supervisory Authorities via the competent Supervisory Authority with a brief explanation of the reasons justifying the update.

RULE 26 - BCR BINDINGNESS

RULE 26 - The Controller Policy is binding across the Sodexo Group for each BCR member, including their employees.

The BCR are part of the intra-group agreement signed by all Sodexo entities and which makes the BCR legally binding.

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 or returns the entire amount of these Personal Data to a Sodexo entity to which the BCR still apply.

The BCR have been shared with all employees as a new Group Data protection policy and available at any time on the official Sodexo's Intranet and official website.

The standard Sodexo employment contracts include commitments for employees authorized to process Personal Data to ensure confidentiality and comply with the Sodexo data protection policies which include the BCR.

Also, the employees already in place are provided with an individual and separate agreement in order to comply with the Sodexo data protection policies which include the BCR.

In both cases, appropriate disciplinary sanctions or judicial action in accordance with the law can apply in case of non-compliance with such data protection policies.

Where applicable it has been subject to the local work council prior information/consultation where required, to ensure that employees do not only benefit from the BCR Data protection principles but also respect them when processing Personal Data for the purpose of their function.

04

Appendices

- Appendix 1: Definitions
- Appendix 2: Sodexo Global Data Protection Policy
- Appendix 3: Table on Transparency
- Appendix 4: BCR Cooperation Procedure
- Appendix 5: BCR Updating Procedure
- Appendix 6: Global Data Collection and Data Retention Policy (Controller)
- Appendix 7: Global Data Protection Rights Management Policy
- Appendix 8: Description of the material scope of the Controller 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 this Controller Policy 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 organizations or corporations 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.

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

- **Data Exporter** means a Controller, or a Processor (when acting on behalf of another Controller of the Group) 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 Controller 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 - Sodexo Global Data Protection Policy

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

Appendix 3 - Table on transparency

Required Information Type	If Personal Data is collected directly from Data Subjects	If Personal Data is NOT collected directly from Data Subjects
Identity and contact details of the controller and, where applicable, their representatives[12]	X	X
Contact details of the DPO	X	X
Purposes and legal basis for the processing	X	X
Where legitimate interests are the legal basis for the processing, the legitimate interests pursued by the Controller or a third party	X	X
Categories of Personal Data concerned	NOT REQUIRED	X
Details of the transfers to third countries and the relevant safeguards	X	X
The storage period (or if not possible, criteria used to determine that period)	X	X
The rights of the Data Subject to access; rectification; erasure; restriction on processing; objection to processing and portability.	X	X
Where processing is based on consent (or explicit consent), the right to withdraw consent at any time	X	X
The right to lodge a complaint with a supervisory authority	X	X

[12] In case of Controllers based outside the EU.

Whether there is a statutory or contractual requirement to provide this information or whether it is necessary to enter into a contract or whether there is an obligation to provide the information and the possible consequences of failure.	X	NOT REQUIRED
The source from which the Personal Data originate, and if applicable, whether it came from a publicly accessible source.	NOT REQUIRED	X
The existence of automated decision-making, including profiling and, if applicable, meaningful information about the logic used the significance and envisaged consequences of such processing for the Data Subject.	X	X

Appendix 4 - BCR Cooperation Procedure

1. This Cooperation Procedure sets out the way in which Sodexo entities adhering to the BCR 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 make the necessary personnel available for dialogue with the competent Supervisory Authorities.

3. Sodexo entities adhering to the BCR 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 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 communicate without undue delay to the competent Supervisory Authorities any material changes to the BCR in accordance with the Updating Procedure (Appendix 5 of the BCR).

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

8. Upon request, Sodexo entities adhering to the BCR will 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 5 - BCR Updating Procedure

Preamble

1. This Updating Procedure sets out the way in which Sodexo will communicate changes to the BCR to the competent Supervisory Authorities, 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. Sodexo will also provide a brief explanation of the reasons for any communicated material changes to the BCR.

Administrative changes

3. 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

4. Sodexo will communicate without undue delay all changes to the BCR, whether administrative or material in nature, to the Sodexo entities adhering to the BCR.

5. Sodexo will 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

6. The Group Data Protection Officer, with the support of the Group Legal team, will (i) keep a fully updated list of Sodexo entities adhering to the BCR. and (ii) keep track of and record any updates to the BCR and provide the necessary information to the Data Subjects or Supervisory Authorities upon request.

7. Sodexo will 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 6 - Global Data Collection and Data Retention Policy (Controller)

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 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 Controller, follows the principles of the GDPR or any other applicable data protection laws.

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 either a Client or another Sodexo entity.

- **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.

I. Storing Personal Data in compliance with the Storage limitation principle

a. Definition of a Personal Data retention period for each purpose

For each purpose of Personal Data Processing, a limited data retention period is defined.

The data retention periods may differ depending on the purpose of Processing. Such periods must be set considering the purpose of Processing, and taking into account:

- Any local legal requirements imposing a data retention period;
- In the absence of any local legal requirements, Personal Data must be retained for no longer than necessary for the purpose for which it is collected.

The definition of a data retention period is a local process. Indeed, the definition of such period relies first on the requirements of any local law that could set out a retention period (for example, for any HR Processing, the local labor law should be reviewed).

If the local laws do not set out a specific data retention period for the Processing at stake, the concerned business owner has the responsibility to define, together with the Data Protection Single Point of Contact and the IT owner, a specific data retention period that complies with the GDPR and any other applicable data protection laws requirements.

The data retention period set out with the business owner shall ensure that once the purpose for Processing ceases to exist and if there is no legal requirement to retain the Personal Data, Personal Data should be immediately anonymized or deleted.

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

b. Active mode

Personal Data will be accessible to appropriate Sodexo's employees in an active mode during the data retention period on a "need to know" basis.

c. Temporary archive

Personal Data may be temporarily archived with restricted access when the purpose for which it was collected no longer exists:

(a) For the duration of the statute of limitation: defense against a potential or actual or future legal or contractual action raised by third parties including Data subjects; or

(b) To comply with a legal obligation.

d. Longer archive

Personal Data may be stored for longer periods for statistical purposes.

In such case, please contact the Global Data Protection Office or your Local Data Protection Single Point of Contact for prior approval in order to assist you with the following steps:

- Retain only Personal Data which is necessary for statistical purposes;
- Anonymize Personal Data retained in an irreversible way where possible;
- If anonymization is not possible, pseudonymize Personal Data and ensure deletion as soon as the statistical purposes are fulfilled; in addition, archive the pseudonymized data in a separate read-only format and give access only to the relevant personnel on a one-off basis.

e. Erasure

At the end of the data retention period (including active mode and temporary archive), Sodexo will delete or anonymize Personal Data in a secured manner.

If the Personal Data has been subprocessed by a Processor, Sodexo should instruct the Processor to delete or return Personal Data at the latest at the termination date of the contract. Sodexo should require from the Processor that it provides an attestation confirming the good deletion of the Personal Data.

II. Monitoring the effective implementation of the defined data retention periods

Once the appropriate data retention period has been set out for a given Personal Data Processing (either because of a local legal requirement or jointly with a business owner), Sodexo will ensure the monitoring of its implementation by complying with the following steps:

1. Ensure that the appropriate data retention period has been correctly recorded in OneTrust for each Personal Data Processing;
2. Create a data retention working group including the local Data Protection Single Point of Contact, the concerned business owner and the IS&T team to technically implement the data retention period (including active mode and temporary archive);
3. Draft a detailed process including the steps to follow to delete Personal Data and the owner of each action identified in the process by the data retention working group;
4. Gather together with the data retention working group on an annual basis to review if the data retention period is correctly implemented and if Personal Data is correctly archived or deleted.

APPENDIX 1 - INDICATIVE DATA RETENTION SCHEDULE

The data retention period shall be defined on the basis of the Processing concerned. The following data retention periods are based on requirements from various French laws.

	Underlying Purpose	Data Retention
Human Ressources	Administrative management	End of the employment contract + 2 years
	Payroll management	End of the employment contract + 5 years
	Recruitment process	3 years after the last contact with the candidate
	Leave of absence	End of the employment contract + 1 year
	Management of access	Maximum of 3 months
	CCTV Records	Maximum of 1 month
Marketing	Clients and prospects database for marketing purposes	3 years after the last contact with the Data subject
	Clients satisfaction surveys	4 years
IT Security	IT Security management	6 months
Finance	Invoicing management	10 years
	Accounting	10 years

Appendix 7 - Global Data Protection Rights Management Policy

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

Appendix 8 - Description of the material scope of the Controller 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
- Recruitment management	- Job applicants	- Identification data (civil status, identity) - Private life (limited to hobbies and other information included in the resumes) - Professional life - CV, education, degrees, professional training, honors, etc. - Economic and financial situation (e.g., salary expectations)	- Potentially all countries where Sodexo operates, when an EU/EEA Sodexo entity recruits an EU/EEA resident for a role located outside of the EU/EEA.
- 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.)	- Employees - Former employees	- Identification data (civil status, identity) - Private life (emergency point of contact, and information necessary to manage the health insurance contract for all the beneficiaries) - Professional life - Economic and financial situation (banking details for payroll management)	- All countries where Sodexo operates.

		- Connection data (e.g., credentials for authentication purposes, logs/interaction with the relevant IT applications)	
- Accounting and financial management of employees (e.g., expenses management), suppliers/vendors, contractors/subcontractors, clients and related controls and reporting.	- Employees - Clients (current or potential business clients) - Consumers/Beneficiaries (current or potential consumer/beneficiaries) - Suppliers/vendors (business contacts) - Contractors/subcontractors (business contacts)	- Identification data (civil status, identity) - Professional life - Economic and financial situation (banking details for expenses management or invoicing process) - Connection data (e.g., credentials for authentication purposes, logs/interaction with the relevant IT applications	- All countries where Sodexo operates.
- 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)	- Employees - Clients (current or potential business clients) - Consumers/Beneficiaries (current or potential consumer/beneficiaries) - Suppliers/vendors (business contacts) - Contractors/subcontractors (business contacts)	- Identification data (civil status, identity) - Professional life - Economic and financial situation (banking details for expenses management or invoicing process) - Connection data (e.g., credentials for authentication purposes, logs/interaction with the relevant IT applications	- All countries where Sodexo operates.
- Risk Management (internal audit, internal controls etc.)	- Employees - Clients (current or potential business clients)	- Identification data (civil status, identity) - Professional life	- All countries where Sodexo operates.

	- Consumers/Beneficiaries (current or potential consumer/beneficiaries) - Suppliers/vendors (business contacts) - Contractors/subcontractors (business contacts)	- Economic and financial situation (banking details for expenses management or invoicing process) - Connection data (e.g., credentials for authentication purposes, logs/interaction with the relevant IT applications	
- Management of employees' safety (including information and location of employees travelling or working abroad, crisis management)	- Employees - External consultants	- Identification data (civil status, identity) - Private life (private phone number when the employee does not have a professional phone for HLC reasons) - Professional life - Connection data (e.g., credentials for authentication purposes, logs/interaction with the relevant IT applications)	- All countries where Sodexo operates, when an EU/EEA Sodexo employee or external consultant travels or works abroad and when non-EU/EEA Sodexo teams need to access their Personal Data for safety purposes.
- 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	- Employees - External consultants	- 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 operates

- IT support management, including infrastructure management, systems management, and applications	- Employees - External consultants	- 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 operates
- Health and safety management	- Employees - External consultants - Others (visitors, site occupants, etc.)	- Identification data (civil status, identity) - Professional life - Connection data (e.g., credentials for authentication purposes, logs/interaction with the relevant IT applications)	- All countries where Sodexo operates, when non-EU/EEA Sodexo Health & Safety teams need to access EU/EEA Sodexo employee, external consultant or other Data Subject Personal Data for health and safety management purposes.
- Information security management (including, but not limited to, prevention, detection and investigation of security incidents, monitoring of compliance with Sodexo's data security policies)	- Employees - External consultants	- 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 operates
- Client relationship management including performance of our services	- Employees - Clients (current or potential business clients)	- Identification data (civil status, identity) - Private life (e.g., life habits) - Professional life	- All countries where Sodexo operates

and any other business operations	- Consumers/Beneficiaries (current or potential consumer/beneficiaries) - Suppliers/vendors (business contacts) - Contractors/subcontractors (business contacts)	- Economic and financial situation (e.g., banking details of clients but mainly legal entities) - Connection data (e.g., credentials for authentication purposes, logs/interaction with the relevant IT applications) - Sensitive data: dietary preferences or restrictions or allergies which may reveal indirectly health data or religious beliefs.	
- Bids, sales and marketing management	- Employees - Clients (current or potential business clients) - Consumers/Beneficiaries (current or potential consumer/beneficiaries) - Suppliers/vendors (business contacts) - Contractors/subcontractors (business contacts)	- Identification data (civil status, identity) - Private life (personal email address for direct marketing if the data subject consented) - Professional life - Connection data (e.g., credentials for authentication purposes, logs/interaction with the relevant IT applications, cookies	- All countries where Sodexo operates
- Supply management	- Suppliers/vendors (business contacts) - Contractors/subcontractors (business contacts)	- Identification data (civil status, identity) - Economic and financial situation (income, financial situation, fiscal situation, etc.)	- All countries where Sodexo operates

		- Connection data (e.g., credentials for authentication purposes, logs/interaction with the relevant IT applications)	
- Internal and external communication and events management	- Employees - Clients (current or potential business clients) - Consumers/Beneficiaries (current or potential consumer/beneficiaries) - Suppliers/vendors (business contacts) - Contractors/subcontractors (business contacts)	- Identification data (civil status, identity) - Professional life - Connection data (e.g., credentials for authentication purposes, logs/interaction with the relevant IT applications, cookies).	- All countries where Sodexo operates
- Data analytics operations (data analysis in order to have a better understanding and intelligence of our clients or consumers/beneficiaries, suppliers/vendors experiences).	- Clients (current or potential business clients) - Consumers/Beneficiaries (current or potential consumer/beneficiaries) - Suppliers/vendors (business contacts)	- Identification data (civil status, identity) - Professional life - Economic and financial situation (transactional data collected by points of sale etc.) - Connection data (e.g., logs/interaction with the relevant IT applications, IP address)	- All countries where Sodexo operates
- Legal corporate management (including but not limited, legal entities management, management of delegations of power and authority)	- Employees - Clients (current or potential business clients) - Suppliers/vendors (business contacts)	- Identification data (civil status, identity) - Professional life - Connection data (e.g., credentials for	- All countries where Sodexo operates

	- Contractors/subcontractors (business contacts)	authentication purposes, logs/interaction with the relevant IT applications)	
- Implementation of ethics and compliance processes (in order to comply with the applicable requirements)	- Employees - Clients (current or potential business clients) - Consumers/Beneficiaries (current or potential consumer/beneficiaries) - Suppliers/vendors (business contacts) - Contractors/subcontractors (business contacts)	- Identification data (civil status, identity) - Professional life - Economic and financial situation (e.g., expenses or invoices review for investigating conflict checks, compliance with the Group gift policy) - Connection data (e.g., credentials for authentication purposes, logs/interaction with the relevant IT applications)	- All countries where Sodexo operates

04 Appendices