Nestlé Good food, Good life

Nestlé
Controller Binding Corporate Rules

NESTLÉ – CONTROLLER BINDING CORPORATE RULES

Introduction

At Nestlé, our values are rooted in respect: respect for ourselves and respect for others, including respect for the privacy of individuals. This commitment to privacy is reflected in the Nestlé Corporate Business Principles. Through this commitment, we, as Nestlé, strive to be worthy of trust for our privacy practices and to succeed in the digital reality by living up to the changing expectations of our stakeholders.

As part of these efforts to protect Personal Data and privacy, Nestlé has implemented these Controller Binding Corporate Rules ("Controller BCRs"). These Controller BCRs are binding on all In-Scope Nestlé Affiliates and their Personnel worldwide, with respect to the Processing of Relevant Personal Data. They are designed to provide adequate protection for the Processing of Relevant Personal Data.

At Nestlé, we are committed to compliance with these Controller BCRs, in order to ensure that all Processing of Relevant Personal Data by, or on behalf of, In-Scope Nestlé Affiliates is fair and lawful.

1 Scope

1.1 Geographical scope: These Controller BCRs apply to the following transfers of Relevant Personal Data:

(a) any transfer of Relevant Personal Data from a Data Exporter to a Data Importer;

(b) any transfer of Relevant Personal Data from a Data Exporter to an In-Scope Nestlé Processor located in a Third Country (provided that the In-Scope Nestlé Controller and the In-Scope Nestlé Processor also enter into a binding agreement that imposes terms consistent with the requirements of Article 28 of the GDPR with respect to the Processing of Relevant Personal Data); and

(c) Onward Transfers, as set out in Clause 20.

Nestlé France has agreed to act as the representative of Nestlé S.A. in the EEA, for all purposes connected with these Controller BCRs, and will act as the EEA-based In-Scope Nestlé Controller with delegated data protection responsibilities. It is the duty of all In-Scope Nestlé Affiliates, and all Nestlé Personnel, to ensure that they abide by the applicable requirements of these Controller BCRs.

1.2 Material scope: These Controller BCRs do not apply to all Personal Data Processed by In-Scope Nestlé Affiliates. Rather, these Controller BCRs are applicable only to Relevant Personal Data (i.e., Personal Data that is transferred under these Controller BCRs – see the definition of "Relevant Personal Data" in Appendix 1). Personal Data that is not within the definition of Relevant Personal Data is not subject to these Controller BCRs. For example, to the extent that an In-Scope Nestlé Controller outside the EEA Processes the Personal Data of local contract workers in accordance with local employment law, and does not

transfer that Personal Data internationally, that Personal Data is not subject to these Controller BCRs.

2 Definitions

Defined terms used in these Controller BCRs are set out in Appendix 1.

3 Lawful, fair and transparent Processing

In-Scope Nestlé Affiliates shall ensure that Relevant Personal Data is Processed lawfully, fairly and in a transparent manner in relation to the Data Subject, and in accordance with the provisions of these Controller BCRs.

4 Secure Processing

Each In-Scope Nestlé Affiliate shall Process Relevant Personal Data in a manner that ensures appropriate security of the Relevant Personal Data in accordance with Clause 17, including by ensuring protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5 Purpose limitation

Relevant Personal Data is only transferred and otherwise Processed by In-Scope Nestlé Affiliates for specific and legitimate purposes. The relevant purposes are set out in Section 2 of Appendix 2. In-Scope Nestlé Affiliates shall ensure that Personal Data will not be further Processed in a manner incompatible with the purposes for which it is collected.

6 Data minimisation

Each In-Scope Nestlé Affiliate will ensure that Relevant Personal Data Processed by it, or by any Processor acting on its behalf, is adequate, relevant and limited to what is necessary in relation to the purposes for which that Relevant Personal Data is Processed.

7 Data retention

Each In-Scope Nestlé Affiliate will:

(a) ensure that Relevant Personal Data Processed by it, or by any Processor acting on its behalf, is kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the Relevant Personal Data is Processed; and

(b) ensure that it abides by the requirements of the Nestlé Record Retention Rules, including by implementing a Retention Schedule, as set out in Exhibit A to those Rules.

8 Data quality and proportionality

Each In-Scope Nestlé Affiliate will ensure that Relevant Personal Data Processed by it, or by any Processor acting on its behalf, is:

(a) accurate and where necessary, kept up to date;

(b) adequate, relevant, and limited to what is necessary for the purposes for which the Relevant Personal Data is transferred or otherwise Processed; and

(c) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Relevant Personal Data is Processed.

9 Legal basis for Processing Relevant Personal Data

In-Scope Nestlé Controllers will only Process Relevant Personal Data (and will only instruct their Processors to Process Relevant Personal Data) on one or more of the following legal bases:

(a) Consent: consent, either explicit or implicit, can be used as a basis for the Processing of Relevant Personal Data, subject to the following conditions:

(i) consent is to be given voluntarily and based on adequate information, and remains valid for so long as there is no Material Change to the circumstances under which it was given;

(ii) In-Scope Nestlé Controllers will be able to demonstrate that the Data Subject has consented to the Processing;

(iii) if the Data Subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language (and any part of such declaration that constitutes an infringement of these Controller BCRs, or of the GDPR, shall not be binding);

(iv) In-Scope Nestlé Controllers are to provide Data Subjects with the ability to withdraw their consent at any time and it must be as easy for Data Subjects to withdraw consent as it is to give consent;

(v) prior to giving consent, the Data Subject shall be informed of the right to withdraw consent, in accordance with Clause 11.2(n); and

(vi) the performance of a contract by In-Scope Nestlé Controllers, including the provision of a service, shall not be conditional on consent to the Processing of Relevant Personal Data that is not necessary for the performance of that contract.

(b) Legitimate interests: an In-Scope Nestlé Controller may Process Relevant Personal Data if it has a Legitimate Interest in carrying out the Processing, and is satisfied that the Processing is permitted under applicable law. Legitimate Interest is generally used for the Processing of Relevant Personal Data of Nestlé Personnel (to the extent that contractual necessity does not apply), and Personnel of Customers and Vendors. Such Legitimate Interests include: research and development; fraud detection; IT security network protection; management of the internal employee directory; charitable

activities; Personnel training; recruitment; and establishment, exercise, or defence of legal claims.

(c) Contractual necessity: Relevant Personal Data may be Processed if it is needed for the performance of a contract between an In-Scope Nestlé Controller and a Data Subject (e.g., for the Processing of Personal Data of Personnel under employment contracts; or where a Consumer makes a purchase from Nestlé, Nestlé may Process the Consumer's Personal Data to fulfil the contract and deliver the product).

(d) Compliance with laws: Relevant Personal Data may be Processed if it is necessary for compliance with a legal obligation to which the In-Scope Nestlé Controller is subject (e.g., in response to a court order).

(e) Vital interests: Relevant Personal Data may be Processed if it is necessary for the vital interests of the Data Subject, or of other persons, where the Data Subject is physically or legally incapable of giving consent.

Any In-Scope Nestlé Affiliate that wishes to rely on a given legal basis is responsible for ensuring that the requirements of that legal basis are satisfied in the circumstances.

10 Legal basis for Processing Relevant Sensitive Personal Data

All requirements that apply to Relevant Personal Data also apply to Relevant Sensitive Personal Data. Relevant Sensitive Personal Data shall not be Processed unless one of the following situations applies:

(a) the Data Subject has given his/her explicit consent to the Processing, except that, to the extent that the laws of a Member State prohibit any particular Processing activity, the consent of the Data Subject will not waive or override any such prohibition;

(b) the Processing is necessary in the context of employment law or laws relating to social security and social protection;

(c) the Processing is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent;

(d) the Processing relates to Relevant Sensitive Personal Data which is manifestly made public by the Data Subject; or

(e) the Processing is necessary for the purpose of establishing, exercising or defending legal claims.

11 Transparency and information rights

11.1 The In-Scope Nestlé Affiliates will ensure that Data Subjects are provided with the information required under Articles 12, 13 and 14 of the GDPR (the full text of these Articles can be found at Appendix 4), by making a full description of the relevant portions of these Controller BCRs available to Data Subjects, through internal and external privacy notices and, where appropriate, through hard copy privacy notices, available on request.

11.2 In addition, In-Scope Nestlé Controllers will ensure that Data Subjects are provided with appropriate information, to be provided in the local language(s) of each Market, regarding the Processing of Relevant Personal Data about them, including:

(a) the In-Scope Nestlé Controller(s) responsible for the Processing of their Relevant Personal Data;

(b) the contact details of the Group Data Protection Officer and, where appropriate, the local Data Protection Champion;

(c) the purposes for which the Relevant Personal Data is Processed, and the legal basis for such Processing;

(d) where the Processing is based on point (f) of Article 6(1) of the GDPR, the Legitimate Interests pursued by the In-Scope Nestlé Controller;

(e) the recipients or categories of recipients of the Relevant Personal Data;

(f) the fact that cross-border transfers of Relevant Personal Data will be made under these Controller BCRs, and the means by which to obtain a copy of these Controller BCRs as set out in Clause 11.4;

(g) the period for which the Relevant Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

(h) an explanation of the rights that Data Subjects may have, subject to applicable law, including the rights of access, rectification, erasure, restriction of Processing, data portability, and an explanation of how Data Subjects can exercise those rights, including the right to lodge a complaint with a supervisory authority;

(i) whether the provision of Relevant Personal Data is a legal or contractual requirement, and an explanation of the possible consequences of failure to provide such data;

(j) where applicable, information on the existence of any automated Processing (including profiling) which produces legal effects concerning Data Subjects, or similarly significantly affects Data Subjects;

(k) information regarding the scope and application of the Controller BCRs, and the application of the general data protection principles (including purpose limitation (see Clause 5), data minimisation (see Clause 6), limited storage periods (including the criteria for determining the period for which Relevant Personal Data will be retained – see Clause 7), data quality (see Clause 8), data protection by design and by default (see Clause 16.1), legal basis for Processing (see Clause 9), Processing of Relevant Sensitive Personal Data (see Clauses 10 and 17.3), measures to ensure data security (see Clause 17), and the requirements in respect of Onward Transfers to bodies not bound by the Controller BCRs (see Clause 20));

(l) information on Nestlé's complaints handling mechanism (see Clause 25);

(m) any further information necessary to make the Processing fair and lawful (including compliance with any additional information rights under any applicable local laws); and

(n) where the Processing of Relevant Personal Data is based on consent, clear information regarding the right to withdraw such consent without affecting the lawfulness of Processing based on consent before its withdrawal.

11.3 In-Scope Nestlé Controllers will provide this information through publicly available online privacy notices and, where appropriate, through hard copy privacy notices, available on request.

11.4 The full text of these Controller BCRs shall be made publicly available at www.nestle.com/bcr. In addition, the full text of these Controller BCRs shall be available on request to the Group Data Protection Officer, either:

(i) by postal mail to: Nestlé S.A., Data Protection Officer, 1800 Vevey, Switzerland; or

(ii) by email to: dataprotectionoffice@nestle.com

12 Rights of Data Subjects

12.1 In-Scope Nestlé Controllers will, in accordance with Articles 12(1) to 12(6) of the GDPR (the full text of which can be found at Appendix 4) and subject to the applicable exemptions set out in the GDPR, implement appropriate technical and organisational measures to enable Data Subjects to exercise the following rights in respect of the transfer and other Processing of their Relevant Personal Data:

(a) where applicable, the right not to provide their Relevant Personal Data to any In-Scope Nestlé Controller;

(b) the right to request access to, or copies of, their Relevant Personal Data, together with:

(i) the purposes of the Processing;

(ii) the categories of Relevant Personal Data concerned;

(iii) the recipients or categories of recipient to whom the Relevant Personal Data has been or will be disclosed, in particular recipients in Third Countries or international organisations;

(iv) where possible, the envisaged period for which the Relevant Personal Data will be retained, or, if not possible, the criteria used to determine that period;

(v) the existence of the right to request rectification or erasure of Relevant Personal Data or restriction of Processing of Relevant Personal Data concerning the Data Subject or to object to such Processing;

(vi) the right to lodge a complaint with a Supervisory Authority;

(vii) where the Relevant Personal Data has not been collected from the Data Subject, any available information as to the source;

(viii) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject (see Clause 13 for further detail on Nestlé's use of automated decision-making); and

(ix) the appropriate safeguards in place to protect the international transfer of their Relevant Personal Data under these Controller BCRs,

and where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the information set out above will be provided securely and in a commonly used electronic form;

(c) the right to request rectification of any inaccuracies in their Relevant Personal Data, and the right to have incomplete Relevant Personal Data completed, including by means of providing a corrective supplementary statement;

(d) the right to request erasure of their Relevant Personal Data where one of the following grounds applies:

(i) the Relevant Personal Data is no longer necessary in relation to the purposes for which it was collected or otherwise Processed (and where the In-Scope Nestlé Controller has made the Relevant Personal Data public and is obliged to erase such Relevant Personal Data pursuant to this paragraph, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform Controllers which are Processing the Relevant Personal Data that the Data Subject has requested the erasure by such Controllers of any links to, or copy or replication of, that Relevant Personal Data);

(ii) the Data Subject withdraws consent to Processing (where this is the legal basis relied upon by the In-Scope Nestlé Controller to Process Relevant Personal Data in accordance with Clause 9(a) and/or Clause 10(a)) and where there is no other legal ground for the Processing;

(iii) the Data Subject objects to the Processing and there are no overriding legitimate grounds for the Processing, or the Data Subject objects to the Processing for direct marketing purposes;

(iv) the Relevant Personal Data has been unlawfully Processed;

(v) the Relevant Personal Data must be erased in order to comply with a legal obligation to which the In-Scope Nestlé Controller is subject; or

(vi) the Relevant Personal Data has been collected in relation to the offer of information society services directly to a child;

(e) the right to request restriction of Processing of their Relevant Personal Data where one of the following applies:

(i) the accuracy of the Relevant Personal Data is contested by the Data Subject, for a period enabling the In-Scope Nestlé Controller to verify the accuracy of the Relevant Personal Data;

(ii) the Processing is unlawful, and the Data Subject opposes the erasure of the Relevant Personal Data and requests the restriction of its use instead;

(iii) the In-Scope Nestlé Controller no longer needs the Relevant Personal Data for the purposes of the Processing, but the Relevant Personal Data is required by the Data Subject for the establishment, exercise or defence of legal claims; or

(iv) the Data Subject has objected to the Processing, pending verification whether the legitimate grounds of the In-Scope Nestlé Controller override those of the Data Subject,

and the In-Scope Nestlé Controller shall communicate any rectification or erasure of Relevant Personal Data or restriction of Processing carried out in accordance with this Clause 12.1 to each recipient to whom the Relevant Personal Data has been disclosed, unless this proves impossible or involves disproportionate effort, and shall inform the Data Subject about those recipients if the Data Subject requests it;

(f) the right to object to the Processing of their Relevant Personal Data by In-Scope Nestlé Controllers where such Processing is based on the Legitimate Interests legal basis set out in Clause 9(b), and/or where the objection relates to direct marketing, to the extent applicable in each case, and subject to the following requirements:

(i) following receipt of an objection request from a Data Subject, an In-Scope Nestlé Controller shall no longer Process the Personal Data unless it can demonstrate compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject, or for the establishment, exercise or defence of legal claims;

(ii) where a Data Subject objects to Processing for direct marketing purposes, the Personal Data shall no longer be Processed for such purposes; and

(iii) In-Scope Nestlé Controllers will clearly and specifically bring the right to object to the attention of Data Subjects, separately to other information;

(g) the right to receive Relevant Personal Data that Data Subjects have provided to In-Scope Nestlé Controllers, or to have such Relevant Personal Data transferred to another Controller, in a structured, commonly used and machine-readable format, to the extent that such Relevant Personal Data is Processed by the In-Scope Nestlé Controllers on the basis of consent (as set out in Clause 9(a) or Clause 10(a)) or contractual necessity (as set out in Clause 9(c));

(h) where Relevant Personal Data is transferred or Processed on the basis of consent, the right to withdraw that consent; and

(i) the right to lodge complaints with a Supervisory Authority regarding the transfer or Processing of their Relevant Personal Data, and to claim compensation for breaches of the Controller BCRs, as further detailed in Clause 26.

12.2 If an In-Scope Nestlé Processor receives a request to exercise any of these rights, it will forward that request to the relevant In-Scope Nestlé Controller.

12.3 Where the relevant In-Scope Nestlé Controller(s) have reasonable doubts concerning the identity of the Data Subject making the request, the relevant In-Scope Nestlé Controller(s) may request the provision of additional information necessary to confirm the identity of the Data Subject. Where a request requires the establishment of additional facts (e.g., a determination of whether any Processing is non-compliant with applicable law) In-Scope Nestlé Controllers will investigate the request reasonably promptly, before deciding what action to take, and will provide the necessary information to the Data Subject without undue delay and in any event within one month of receipt of the request. This period may be extended by two further months where necessary, taking into account the complexity and number of requests. The In-Scope Nestlé Controller(s) shall inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

12.4 Data Subjects may contact In-Scope Nestlé Affiliates for the purposes of exercising any of these rights, using the "contact us" form on the Nestlé website which can be found at https://www.nestle.com/bcr, or through any other means made available by the local Nestlé Affiliate.

13 Automated decision-making

13.1 In-Scope Nestlé Affiliates will not make evaluations or decisions relating to Relevant Personal Data based solely on automated Processing, which produce legal effects concerning Data Subjects, or similarly significantly affect Data Subjects, unless the relevant evaluation or decision:

(a) is necessary for entering into, or performance of, a contract between the Data Subject and the In-Scope Nestlé Controller;

(b) is required or permitted by applicable EU or Member State law to which the In-Scope Nestlé Affiliates are subject, and which implements suitable safeguards to protect the rights and freedoms and legitimate interests of Data Subjects; or

(c) is based on the explicit consent of the Data Subject.

13.2 Where an evaluation or decision is made under Clause 13.1(a) or 13.1(c), In-Scope Nestlé Affiliates will provide the Data Subject with 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.

14 Demonstration of compliance

14.1 Each In-Scope Nestlé Affiliate must ensure that it is able to demonstrate that it is in compliance with its obligations under these Controller BCRs. In order to demonstrate

compliance, In-Scope Nestlé Affiliates will maintain a record of all categories of Processing activities in respect of Relevant Personal Data. This record must be implemented in writing, including in electronic form, and in a format that complies with the requirements of Article 30 of the GDPR. Each In-Scope Nestlé Affiliate will make available the record described in this Clause 14 to a Supervisory Authority on request.

14.2 The record specified in Clause 14.1 will contain all of the following information:

(a) the name and contact details of the In-Scope Nestlé Controller and, where applicable any joint controllers, the In-Scope Nestlé Controller's representative, and the Group Data Protection Officer;

(b) the purposes of the Processing;

(c) a description of the categories of Data Subjects and of the categories of Relevant Personal Data;

(d) the categories of recipients to whom the Relevant Personal Data have been or will be disclosed including recipients in Third Countries or international organisations;

(e) where applicable, transfers of Relevant Personal Data to a Third Country or an international organisation, including the identification of that Third Country or international organisation and documentation of the suitable safeguards or derogations relied upon to safeguard such transfers;

(f) where possible, the envisaged time limits for erasure of the different categories of Relevant Personal Data; and

(g) where possible, a general description of the technical and organisational security measures in place to protect Relevant Personal Data (such measures shall be in accordance with Clause 17).

14.3 The record for In-Scope Nestlé Processors will contain all of the following information:

(a) the name and contact details of the In-Scope Nestlé Processor and of each In-Scope Nestlé Controller on behalf of which the In-Scope Nestlé Processor is acting, and, where applicable, of the In-Scope Nestlé Controller's or the In-Scope Nestlé Processor's representative, and the Group Data Protection Officer;

(b) the categories of Processing carried out on behalf of each In-Scope Nestlé Controller; and

(c) where applicable, transfers of Relevant Personal Data to a Third Country or an international organisation, including the identification of that Third Country or international organisation and documentation of the suitable safeguards or derogations relied upon to safeguard such transfers; and

(d) where possible, a general description of the technical and organisational security measures in place to protect Relevant Personal Data (such measures shall be in accordance with Clause 17).

15 Data Protection Impact Assessments

15.1 A Data Protection Impact Assessment must be completed for:

(a) each new Processing system that Processes Relevant Personal Data during the design phase, and must be updated for all systems on an annual basis; and

(b) each change to an existing Processing system that Processes Relevant Personal Data, where such change is likely to result in a high risk to the rights and freedoms of Data Subjects.

15.2 Data Protection Impact Assessments will be required in particular where Processing of Relevant Personal Data involves:

(a) 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;

(b) Processing on a large scale of Sensitive Personal Data, or of Relevant Personal Data relating to criminal convictions and offences or related security measures;

(c) a systematic monitoring of a publicly accessible area on a large scale;

(d) cross-referencing or combining datasets containing Relevant Personal Data;

(e) vulnerable Data Subjects;

(f) innovative use or applying new technological or organisational solutions; or

(g) preventing Data Subjects from exercising a right or using a service or contract.

15.3 Supervisory Authorities may publish their own lists of Processing activities which will necessitate In-Scope Nestlé Affiliates to carry out a Data Protection Impact Assessment. These lists may complement or specify further criteria to those set out in Clause 15.2 above. In-Scope Nestlé Affiliates shall therefore assess and comply with the requirements of applicable law in advance of conducting a Data Protection Impact Assessment on a case-by-case basis.

15.4 In-Scope Nestlé Affiliates will seek the advice of the Group Data Protection Officer when carrying out a Data Protection Impact Assessment.

15.5 Where a Data Protection Impact Assessment indicates that the relevant Processing activity would result in a high risk to the rights, freedoms or interests of Data Subjects, the relevant In-Scope Nestlé Affiliates should implement appropriate measures to mitigate the risks. If such measures cannot be implemented, the Concerned Supervisory Authorities should be consulted prior to the commencement of the relevant Processing activity.

15.6 As part of the Data Protection Impact Assessment, In-Scope Nestlé Affiliates should pay particular attention to ensuring that the Processing of Relevant Personal Data is limited to what is necessary to achieve the relevant purposes.

16 Data protection by design and by default

16.1 In-Scope Nestlé Affiliates will implement appropriate technical and organisational measures designed to implement the data protection principles set out in these Controller BCRs and to facilitate compliance with the requirements of these Controller BCRs. Such measures will include:

(a) 'data protection by design' (i.e., the In-Scope Nestlé Affiliate will, in the course of designing and implementing any new Processing activity involving Relevant Personal Data, ensure that it has included in the design for that Processing activity suitable safeguards and mechanisms to ensure compliance with the requirements set out in these Controller BCRs, including limiting the Processing of Relevant Personal Data to what is necessary to achieve the relevant purposes); and

(b) 'data protection by default' (i.e., the In-Scope Nestlé Affiliate will, whenever it embarks on a new Processing activity, ensure that, by default, only Relevant Personal Data that is necessary for that activity is Processed).

17 Security and confidentiality

17.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, In-Scope Nestlé Affiliates will implement appropriate technical and organisational measures to protect Relevant Personal Data against unauthorised, accidental or unlawful destruction, loss, alteration, misuse, disclosure or access and against all other unlawful forms of Processing ("Security Measures"). To this end, In-Scope Nestlé Affiliates must comply with all Group IS/IT Security Standards, policies and procedures, and must ensure that any third party Processors or other subcontractors will also adhere to principles consistent with the applicable Group IS/IT Security Standards when Processing Relevant Personal Data.

17.2 The Security Measures will include, as appropriate:

(a) the pseudonymisation and encryption of Relevant 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 Relevant 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 organisational measures for ensuring the security of the Processing; and

(e) the measures set out in Appendix 5.

17.3 In particular, In-Scope Nestlé Affiliates will ensure that Relevant Sensitive Personal Data is Processed with appropriate enhanced Security Measures (including encryption or pseudonymisation where practicable).

18 Personal Data Breach reporting

18.1 In-Scope Nestlé Affiliates will:

(a) implement the Nestlé Data Breach Response Plan and follow the provisions of that Plan with respect to the identification, assessment, documentation and reporting of Personal Data Breaches;

(b) ensure that their respective Personnel receive appropriate training, in accordance with Clause 21, to enable them to adhere to the Nestlé Data Breach Response Plan;

(c) in accordance with the Nestlé Reporting Information Security Events Process ("RISE"), report Personal Data Breaches (including the relevant facts, the effects of the breach and any remediation steps taken) to the Security Operations Centre. Where required under the Nestlé Internal Practice Personal Data Breach Response Procedure, the Security Operations Centre will report to the Group Data Protection Officer using the contact details provided in Clause 25 below;

(d) make available the Nestlé Data Breach Response Plan, the GLOBE Standard Response Procedure for Personal Data Breaches, and any relevant records or other supporting documents relating to any particular Personal Data Breach, on demand, to any Concerned Supervisory Authority; and

(e) when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of Data Subjects, communicate the Personal Data Breach to the Data Subjects without undue delay.

18.2 In the event that a Personal Data Breach reported in accordance with this Clause 18 is assessed under the Nestlé Data Breach Response Plan to have resulted in a risk to the rights and freedoms of Data Subjects, such Personal Data Breach will be reported to the Concerned Supervisory Authority without undue delay and, where feasible, within 72 hours of the Personal Data Breach having been identified. Where the notification referred to in this Clause 18.2 is not made within 72 hours, the notification shall be accompanied by reasons for the delay.

18.3 The "relevant records" referred to in Clause 18.1(d) shall include:

(a) the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Relevant Personal Data records concerned;

(b) the name and contact details of the Group Data Protection Officer or other contact point where more information can be obtained;

(c) the likely consequences of the Personal Data Breach; and

(d) the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

19 Relationship with Processors

For the purposes of Processing Relevant Personal Data received under these Controller BCRs, In-Scope Nestlé Controllers may engage Processors in two scenarios:

(a) where an In-Scope Nestlé Controller engages an In-Scope Nestlé Processor to Process any Relevant Personal Data on its behalf, the In-Scope Nestlé Controller will ensure that the Processing of the Relevant Personal Data is subject to the terms of these Controller BCRs, together with an agreement that imposes terms consistent with the requirements of Article 28 of the GDPR with respect to the Processing of Relevant Personal Data; and

(b) where an In-Scope Nestlé Controller engages an entity as a Processor to Process any Relevant Personal Data on its behalf, and that Processor is either:

(i) not a Nestlé Affiliate; or

(ii) a Nestlé Affiliate but not an In-Scope Nestlé Processor,

then, in addition to the requirements of Clause 20.1(c), the In-Scope Nestlé Controller will, prior to disclosing the Relevant Personal Data to such Processor, enter into a binding agreement with such Processor that imposes terms consistent with the requirements of Article 28 of the GDPR with respect to the Processing of Relevant Personal Data.

20 Restrictions on Onward Transfers

20.1 In-Scope Nestlé Affiliates are not permitted to perform Onward Transfers of Relevant Personal Data, except in accordance with the following conditions:

(a) Onward Transfers to In-Scope Nestlé Controllers: An In-Scope Nestlé Controller that received the Relevant Personal Data under these Controller BCRs may perform an Onward Transfer of the same Relevant Personal Data to another In-Scope Nestlé Controller, provided that such transfer is performed in compliance with these Controller BCRs.

(b) Onward Transfers to In-Scope Nestlé Processors: In accordance with Clause 19(a), an In-Scope Nestlé Controller that received the Relevant Personal Data under these Controller BCRs may perform an Onward Transfer of the same Relevant Personal Data to an In-Scope Nestlé Processor, provided that such transfer takes place under these Controller BCRs, together with an agreement that imposes terms consistent with the requirements of Article 28 of the GDPR with respect to the Processing of Relevant Personal Data.

(c) Onward Transfers to Processors (other than In-Scope Nestlé Processors): An In-Scope Nestlé Controller may perform an Onward Transfer of Relevant Personal Data to a

Processor that is either: (i) not a Nestlé Affiliate; or (ii) a Nestlé Affiliate but not an In-Scope Nestlé Processor; provided that:

1) where required, the In-Scope Nestlé Controller has ensured that at least one of the safeguards or derogations for the transfer of Personal Data to Third Countries (set out in Articles 44-49 of the GDPR) applies;

2) the In-Scope Nestlé Controller has assessed whether there is anything in the law or practice of the Processor that may impinge on the effectiveness of the appropriate safeguards relied upon, and shall identify and adopt supplementary measures that are necessary to bring the level of protection of the Relevant Personal Data transferred up to the standard required by the GDPR, as appropriate; and

3) as set out in Clause 19(b) the In-Scope Nestlé Controller enters into a binding agreement with the Processor that imposes terms consistent with the requirements of Article 28 of the GDPR with respect to the Processing of Relevant Personal Data.

(d) Onward Transfers to third party Controllers: An In-Scope Nestlé Controller may perform an Onward Transfer of Relevant Personal Data to a third party Controller only if:

(i) where required, the In-Scope Nestlé Controller has ensured that at least one of the safeguards or derogations for the transfer of Personal Data to Third Countries (set out in Articles 44-49 of the GDPR) applies;

(ii) the In-Scope Nestlé Controller has assessed whether there is anything in the law or practice of the Processor that may impinge on the effectiveness of the appropriate safeguards relied upon, and shall identify and adopt supplementary measures that are necessary to bring the level of protection of the Relevant Personal Data transferred up to the standard required by the GDPR, as appropriate; and

(iii) the In-Scope Nestlé Controller enters into a binding agreement with the third party Controller that imposes on that third party Controller terms that are at least as protective as the requirements of these Controller BCRs.

(e) Onward Transfers to Nestlé sub-Processors: An In-Scope Nestlé Processor may perform an Onward Transfer of Relevant Personal Data to another In-Scope Nestlé Processor provided that such transfer takes place under these Controller BCRs in accordance with the instructions of the relevant Controller.

(f) Onward Transfers to third party sub-Processors: An In-Scope Nestlé Processor may perform an Onward Transfer of Relevant Personal Data to a third party Processor, provided that:

(i) the Onward Transfer has been approved by the relevant In-Scope Nestlé Controller;

(ii) the In-Scope Nestlé Controller has assessed whether there is anything in the law or practice of the Processor that may impinge on the effectiveness of the appropriate safeguards relied upon, and shall identify and adopt supplementary measures that are necessary to bring the level of protection of the Relevant Personal Data transferred up to the standard required by the GDPR, as appropriate; and

(iii) the In-Scope Nestlé Controller enters into a binding agreement with the third party Processor that imposes on that third party Processor terms that are at least as protective as the requirements of these Controller BCRs, and an obligation on the sub-Processor to document all Personal Data Breaches affecting Relevant Personal Data, and notify such Personal Data Breaches to Nestlé France without undue delay.

20.2 In relation to any Onward Transfer of Relevant Personal Data, the In-Scope Nestlé Affiliate responsible for initiating that Onward Transfer will record in the agreement governing the Onward Transfer (or, if there is no such agreement, in an internal written record) which of the safeguards and derogations set out in Articles 44-49 of the GDPR applies to that Onward Transfer.

21 Training program

All In-Scope Nestlé Affiliates must ensure that any Personnel with permanent or regular access to Relevant Personal Data must be provided with adequate training. In-Scope Nestlé Affiliates must ensure that any global training provided by the Group Data Protection Office is mandatory for all such Personnel, and is designed to equip such Personnel with an understanding of their respective responsibilities in relation to the Processing of Relevant Personal Data. Nestlé global training may also be supplemented by local training as necessary.

22 Audits

22.1 All In-Scope Nestlé Affiliates are subject to audits in respect of their compliance with all applicable aspects of these Controller BCRs, on the following terms:

(a) Audit by internal or external auditors: Each In-Scope Nestlé Affiliate accepts that its compliance with these Controller BCRs may be audited by an internal or external auditor appointed by Nestlé S.A., at any time, upon request of the Head of Nestlé Corporate Audit or the Group Data Protection Officer. Such audits will cover:

(i) the digital systems used to Process Relevant Personal Data;

(ii) the physical security of the relevant premises;

(iii) the processes and procedures applicable to Nestlé Personnel who Process Relevant Personal Data;

(iv) decisions taken as regards any mandatory requirement under national laws that conflicts with the Controller BCRs;

(v) implementation of appropriate data Processing agreements where Processors are appointed; and

(vi) the existence and application of suitable corrective measures.

The audit program covers all aspects of these Controller BCRs. In the event that an audit identifies any material non-compliance with the principles set out in these Controller BCRs, the relevant In-Scope Nestlé Affiliate that is found to be non-compliant will promptly implement the necessary corrective actions to achieve compliance.

The Concerned Supervisory Authorities may obtain, on request to the Group Data Protection Officer, a copy of the most recent audit report.

(b) Audit by the CNIL and other Concerned Supervisory Authorities: Each In-Scope Nestlé Affiliate acknowledges that the CNIL, and any other Concerned Supervisory Authority, will have the power to conduct their own data protection audits, for the purposes of establishing compliance with these Controller BCRs.

(c) Self-audits: Each In-Scope Nestlé Affiliate will conduct an audit of its own compliance with its obligations under these Controller BCRs at least once every twenty-four (24) months.

22.2 In the event that an In-Scope Nestlé Affiliate is subject to any of the audits set out in Clause 22.1, the auditor will ensure that the results of the relevant audit(s) are systematically communicated to the Data Protection Champion and the board of the relevant In-Scope Nestlé Affiliate and the Group Data Protection Officer. The Group Data Protection Officer may decide to escalate such audit results to the Compliance Committee and/or the executive board of Nestlé S.A.

23 Compliance and supervision of compliance

23.1 Nestlé has created, and will maintain, the following data protection compliance structure:

(a) each In-Scope Nestlé Affiliate accepts responsibility for ensuring that its own Personnel abide by the terms of these Controller BCRs;

(b) the Data Protection Champion for the In-Scope Affiliate leads the Privacy Program, including these Controller BCRs for his or her respective In-Scope Affiliates;

(c) in the event that the local Data Protection Champion has reason to believe that any member(s) of any Nestlé Personnel have materially breached, or otherwise failed to comply with, these Controller BCRs, he or she can escalate this to the local Compliance Committee and/or the Group Data Protection Officer, who may promptly conduct an investigation into the matter, to determine whether such a breach, or failure to comply, has occurred;

(d) if any Nestlé Personnel are found to have breached, or failed to comply with, these Controller BCRs, the local Market will determine appropriate, effective and dissuasive penalties, up to and including recommending termination of employment; and

(e) the Group Data Protection Officer has ultimate authority over the monitoring of Nestlé's overall compliance with applicable data protection laws, and the Data Protection Champions and the local Compliance Committees are obliged to comply with all recommendations, instructions and decisions related to the Processing of Personal Data issued by the Group Data Protection Officer.

23.2 Each Data Importer shall promptly inform the relevant Data Exporter(s) and the Group Data Protection Officer if it is unable to comply with its respective obligations under these Controller BCRs, for whatever reason.

23.3 Relevant Personal Data that has been transferred under these Controller BCRs shall, in the event of termination of these Controller BCRs, at the choice of the relevant Data Exporter immediately be returned to that Data Exporter, or deleted in its entirety. The same shall apply to any copies of such Relevant Personal Data. In such cases, each affected Data Importer shall certify the deletion of the Relevant Personal Data to the relevant Data Exporter(s). Until the Relevant Personal Data is deleted or returned, each affected Data Importer shall continue to ensure compliance with these Controller BCRs. In case of local laws applicable to an affected Data Importer that prohibit the return or deletion of the transferred Relevant Personal Data, each Data Importer warrants that it will continue to ensure compliance with these Controller BCRs and will only process the Relevant Personal Data to the extent and for as long as required under that local law.

24 Conflicts between the Nestlé Controller BCRs and applicable national laws

24.1 Each In-Scope Nestlé Affiliate warrants that it has no reason to believe that the laws and practices in the Third Country of destination applicable to the Processing of the Relevant Personal Data by the relevant Data Importer, including any requirements to disclose Relevant Personal Data or measures authorising access by public authorities, prevent that Data Importer from fulfilling its obligations under these Controller BCRs. This is based on the understanding that 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 Regulation (EU) 2016/679, are not in contradiction with these Controller BCRs.

24.2 Each In-Scope Nestlé Affiliate declares that in providing the warranty in Clause 24.1, it has taken due account in particular of the following elements:

(a) 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 Relevant Personal Data; the economic sector in which the transfer occurs; the storage location of the Relevant Personal Data transferred;

(b) the laws and practices of the Third Country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards; and

(c) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Controller BCRs, including measures applied during transmission and to the Processing of the Relevant Personal Data in the country of destination.

24.3 Each Data Importer warrants that, in carrying out the assessment under Clause 24.2, it has made its best efforts to provide the relevant Data Exporter with relevant information and agrees that it will continue to cooperate with the relevant Data Exporter in ensuring compliance with these Controller BCRs.

24.4 Each Data Importer shall document the assessment under Clause 24.2, provide a copy to the Group Data Protection Officer in each case, and make it available to the competent Supervisory Authority on request.

24.5 Each Data Importer agrees to notify the relevant Data Exporter(s) and the Group Data Protection Officer promptly if, after having agreed to these Controller BCRs and for the duration of these Controller BCRs, it has reason to believe that it is, or has become, subject to laws or practices not in line with the requirements under Clause 24.1, including following a change in the laws of the Third Country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in Clause 24.1.

24.6 Following a notification pursuant to Clause 24.5, or if the relevant Data Exporter otherwise has reason to believe that the relevant Data Importer can no longer fulfil its obligations under these Controller BCRs, the relevant Data Exporter shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the relevant Data Exporter(s) and/or relevant Data Importer(s) to address the situation. The relevant 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 relevant Data Exporter may terminate these Controller BCRs as between itself and the relevant Data Importer. Where the involvement of any In-Scope Nestlé Affiliate is terminated pursuant to this Clause, Clause 23.3 shall apply.

24.7 Each Data Importer agrees to notify the relevant Data Exporter, the Group Data Protection Officer, and, where possible, the Data Subject promptly (if necessary with the help of the relevant Data Exporter) if it:

(a) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of Relevant Personal Data transferred pursuant to these Controller BCRs; such notification shall include information about the Relevant Personal Data requested, the requesting authority, the legal basis for the request and the response provided; or

(b) becomes aware of any direct access by public authorities to Relevant Personal Data transferred pursuant to these Controller BCRs in accordance with the laws of the country of destination; such notification shall include all information available to the Data Importer.

24.8 If the Data Importer is prohibited from notifying the Data Exporter and/or the Data Subject under the laws of the Third Country of destination, the Data Importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The Data Importer agrees to document its best efforts in order to be able to demonstrate them on request of the Data Exporter.

24.9 Where permissible under the laws of the Third Country of destination, each Data Importer agrees to provide each relevant Data Exporter, at regular intervals for the duration of these Controller BCRs, with as much relevant information as possible on the requests received (in particular, the number of requests, the type of data requested, the requesting Supervisory Authority/ies, whether requests have been challenged, and the outcome of such challenges).

24.10 Each Data Importer agrees to preserve the information pursuant to Clauses 24.7 to 24.9 for the duration of these Controller BCRs and make that information available to the competent Supervisory Authority on request, and to the Group Data Protection Officer in each case.

24.11 Clauses 24.7 to 24.9 are without prejudice to the obligations of the Data Importer pursuant to Clauses 24.5 and 23.2 to inform the relevant Data Exporter and the Group Data Protection Officer promptly where it is unable to comply with these Controller BCRs.

24.12 Each Data Importer agrees to review the legality of any request for disclosure of Relevant Personal Data, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the Third Country of destination, applicable obligations under international law and principles of international comity. Each Data Importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the relevant Data Importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Relevant Personal Data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of each such Data Importer under Clause 24.5.

24.13 Each Data Importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the Third Country of destination, make the documentation available to the relevant Data Exporter and the Group Data Protection Officer on request. Each Data Importer shall also make such assessment available to the competent Supervisory Authority on request.

24.14 Each Data Importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

25 Internal complaints handling mechanism

25.1 Where a Data Subject believes that an In-Scope Nestlé Affiliate is not complying with these Controller BCRs, he or she may complain in writing by contacting that In-Scope Nestlé Affiliate using its published contact details which are available at

https://www.nestle.com/bcr, or the Group Data Protection Officer at Nestlé S.A., Data Protection Officer, 1800 Vevey, Switzerland, or dataprotectionoffice@nestle.com. The complaint should identify the In-Scope Nestlé Affiliate concerned (where possible) describe the alleged breach in as much detail as possible and be accompanied by all relevant documents and evidence (to the extent available).

25.2 The In-Scope Nestlé Affiliate or the Group Data Protection Officer (as appropriate) will resolve the complaint diligently, by acknowledging receipt and investigating it, in accordance with the Internal Complaints Handling Procedure in accordance with the time limits set out in Article 12(3) of the GDPR, as set out in Appendix 4. Where necessary, the matter will be escalated to the relevant Compliance Committee. The In-Scope Nestlé Affiliate or the Group Data Protection Officer (as appropriate) will ensure that the decision regarding the complaint is communicated in writing to the Data Subject as soon as reasonably possible, and in any event in accordance with the time limits set out in Article 12(3) of the GDPR, as set out in Appendix 4.

26 Third party beneficiary rights

26.1 Each Data Subject is entitled to enforce Clauses 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 24, 25, 26, 27 or 28, as the beneficiary of those Clauses.

26.2 Independently of the process set out in Clause 25, any Data Subject who considers that the Processing of Relevant Personal Data relating to him or her by an In-Scope Nestlé Affiliate infringes any of the provisions listed in Clause 26.1, shall be entitled to seek judicial remedies, obtain redress and, where appropriate, seek compensation for material or non-material damage by:

(a) lodging a complaint with the competent Supervisory Authority (and the Data Subject shall be entitled to choose the Supervisory Authority in the EEA Member State of:

(i) his or her habitual residence;

(ii) his or her place of work; or

(iii) the place of the alleged infringement); and/or

(b) without prejudice to paragraph (a) above, lodge a complaint with the competent courts (and the Data Subject shall be entitled to choose the courts of the EEA Member State in which:

(i) the relevant In-Scope Nestlé Affiliate has an establishment; or

(ii) the Data Subject has his or her habitual residence).

Data Subjects are also reminded of their rights under this Clause in Nestlé's privacy notices.

27 Liability

27.1 Each In-Scope Nestlé Controller is responsible for its own compliance with these Controller BCRs.

27.2 If a Data Importer violates these Controller BCRs, the courts or other competent authorities in the EEA will have jurisdiction and Data Subjects will have the rights and remedies against Nestlé France as though the violation had been caused by Nestlé France in France. In accordance with Article 47(2)(f) of the GDPR, Nestlé France accepts liability and responsibility for, and (together with Nestlé S.A., where appropriate) agrees to take the necessary action to:

(a) remedy any actions of Data Importers that are performed in breach of these Controller BCRs; and

(b) pay legally necessary compensation for any material or non-material damage resulting from the violation of these Controller BCRs by such Data Importer.

Nestlé France may, however, demonstrate that the Data Importer is not liable for the violation resulting in the damages claimed by the Data Subject in connection with any alleged breach of these Controller BCRs, in which case it may discharge itself from all responsibility and liability. The burden of proof with respect to such alleged breach of these Controller BCRs will rest with Nestlé France.

28 Mutual assistance and cooperation with Supervisory Authorities

28.1 In-Scope Nestlé Affiliates will provide one another with all reasonable assistance and cooperation in responding to requests and complaints from Data Subjects or investigations or inquiries by any Concerned Supervisory Authority(ies).

28.2 In-Scope Nestlé Affiliates will co-operate with, and accept to be audited by, the Concerned Supervisory Authorities, including as set out in Clause 22.1(b), and to comply with the advice of these Concerned Supervisory Authorities on any issue related to these Controller BCRs.

29 Updates of these Controller BCRs and list of In-Scope Nestlé Affiliate

29.1 Nestlé S.A., in its capacity as the Coordinating Party under the IGA, acting through the Group Data Protection Office, will:

(a) maintain an up-to-date list of all In-Scope Nestlé Affiliates, provide that up-to-date version of the list to Data Subjects or Concerned Supervisory Authority(ies) upon request, and provide that up-to-date version of the list to the CNIL on an annual basis;

(b) maintain an up-to-date version of these Controller BCRs (including all Material Changes) and the IGA and provide such updated version to Concerned Supervisory Authority(ies) upon request;

(c) report all revisions to these Controller BCRs, or the list of In-Scope Nestlé Affiliates, to the CNIL and to the In-Scope Nestlé Affiliates, once per calendar year together with a brief explanation of the reasons justifying any such changes;

(d) promptly report to the CNIL any Material Changes to these Controller BCRs that are likely to:

(i) affect the level of the protection offered by these Controller BCRs; or

(ii) significantly affect the performance, operation or structure of these Controller BCRs;

(e) promptly notify all In-Scope Nestlé Affiliates of any revisions to these Controller BCRs; and

(f) report any Material Changes to these Controller BCRs to Data Subjects, reasonably promptly, through an appropriate notice on Nestlé websites, or by any other available appropriate means.

29.2 In-Scope Nestlé Affiliates undertake not to transfer any Relevant Personal Data on the basis of these Controller BCRs to any new Nestlé Affiliate seeking to become a party to these Controller BCRs until Nestlé S.A. has issued group-wide confirmation in writing that such new Nestlé Affiliate has become bound by the IGA and these Controller BCRs, and the relevant existing In-Scope Nestlé Affiliate is satisfied that such new Nestlé Affiliate will deliver compliance with its obligations under those documents.

30 Relationship between national laws and these Controller BCRs

Where any laws applicable to an In-Scope Nestlé Affiliate require a higher level of protection for Personal Data than the standard set out in these Controller BCRs, such laws will take precedence over these Controller BCRs.

31 Entry into force

These Controller BCRs will enter into force on May 16, 2024, for an indefinite period. All In-Scope Nestlé Affiliates are expected to be in full compliance with these Controller BCRs by no later than six (6) months after the date on which that In-Scope Nestlé Affiliate executed the IGA.

Appendix 1 – Defined Terms

The following defined terms are used in these Controller BCRs:

"CNIL" means the Commission nationale de l'informatique et des libertés (i.e., the Supervisory Authority for France).

"Compliance Committee" means the committee of the relevant Nestlé In-Scope Affiliate with responsibility for compliance measures.

"Concerned Supervisory Authority" means a "supervisory authority concerned" as that term is defined in the GDPR.

"Consumer" means an individual consumer, or potential consumer, of any Nestlé product or service.

"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 accordance with Article 4(7) of the GDPR.

"Coordinating Party" has the meaning given to it in the IGA.

"Customer" means a corporate customer of any Nestlé Affiliate.

"Data Exporter" means an In-Scope Nestlé Affiliate in an EEA Member State that transfers Relevant Personal Data under these Controller BCRs.

"Data Importer" means an In-Scope Nestlé Affiliate in a Third Country that receives Relevant Personal Data under these Controller BCRs.

"Data Protection Champion" means the individual member(s) of Personnel of each Nestlé Affiliate who has been tasked with responsibility for data protection compliance. More than one Nestlé Affiliate may share a Data Protection Champion.

"Data Protection Impact Assessment" means an assessment run for the purpose of evaluating the impact of envisaged Processing operations on the protection of Personal Data, and as further particularised in Article 35 of the GDPR.

"Data Protection Officer" means an officer appointed in accordance with the provisions of Articles 37-39 of the GDPR.

"Data Subject" means a natural person who can be identified, directly or indirectly, by reference to one more categories of Personal Data, in accordance with Article 4(1) of the GDPR.

"EEA" means the European Economic Area (i.e., Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Liechtenstein, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden). For the avoidance of doubt, references to the "EEA" do not include the United Kingdom.

"EU" means the European Union.

"GDPR" means 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).

"Group Data Protection Office" means the Group Data Protection Officer's team, including legal and technical support.

"Group Data Protection Officer" means the Data Protection Officer appointed by Nestlé S.A., acting on behalf of itself, and Nestlé France under power of attorney, tasked with overseeing data protection compliance by Nestlé Affiliates.

"IGA" means the intra-group agreement concluded among all In-Scope Nestlé Affiliates, for the purposes of making these Controller BCRs legally binding upon them.

"In-Scope Nestlé Affiliate" means a Nestlé Affiliate (whether acting as a Controller or a Processor, and whether established within the EEA or in any other part of the world) that is bound by these Controller BCRs and the IGA.

"In-Scope Nestlé Controller" means an In-Scope Nestlé Affiliate that is acting as a Controller with respect to any Relevant Personal Data. (Note that a single In-Scope Nestlé Affiliate may be a Controller for some purposes, and a Processor for others).

"In-Scope Nestlé Processor" means an In-Scope Nestlé Affiliate that is acting as a Processor with respect to any Relevant Personal Data. (Note that a single In-Scope Nestlé Affiliate may be a Controller for some purposes, and a Processor for others).

"Internal Complaints Handling Procedure" means the procedure set out in Appendix 3.

"Legitimate Interest" means a legitimate interest pursued by an In-Scope Nestlé Controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

"Market" means the Nestlé Affiliates within a given jurisdiction.

"Material Change" means a change to these Controller BCRs that is material to the operation or function of these Controller BCRs, or to the rights or obligations set out in these Controller BCRs.

- Examples of changes that are Material Changes include any change to the frequency of audits in Clause 22, or any change to the rights of third party beneficiaries in Clause 26.
- Examples of changes that are not Material Changes include correction of typographical errors, or addresses of Parties.

"Member State" means a Member State of the European Union.

"Nestlé Affiliate" means any entity within the Nestlé group.

"Nestlé France" means Nestlé France SAS, a company established in France, with identification number 542 014 428 R.C.S. Meaux and registered address at 7 Boulevard Pierre Carle, 77186 Noisiel, France.

"Nestlé Record Retention Rules" means the Nestlé Record Retention Rules Standard 2007, as amended from time to time.

"Onward Transfer" means a transfer or disclosure, whether or not across a national border, of Relevant Personal Data, from an In-Scope Nestlé Affiliate that received the Relevant Personal Data under these Controller BCRs, to any recipient of any kind.

"Personal Data" means any information relating to a Data Subject, including an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that Data Subject, in accordance with Article 4(1) of the GDPR.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed, in accordance with Article 4(12) of the GDPR.

"Personnel" means any current, former and prospective directors, officers, consultants, employees, temporary staff, agency workers, individual contractors, interns, secondees, volunteers and other personnel, beneficiaries of personnel benefit plans, and members of pension schemes.

"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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, in accordance with Article 4(2) of the GDPR, and "Process" or "Processed" shall be construed accordingly.

"Processor" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of a Controller, in accordance with Article 4(8) of the GDPR.

"Relevant Personal Data" means Personal Data that is transferred under these Controller BCRs. Categories of Relevant Personal Data are listed in Section 2 of Appendix 2, below.

"Relevant Sensitive Personal Data" means Sensitive Personal Data that is transferred under these Controller BCRs.

"Retention Schedule" means the Retention Schedule set out in Exhibit A to the Nestlé Record Retention Rules.

"Security Measures" has the meaning given to it in Clause 17.1.

"Sensitive Personal Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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, in accordance with Article 9(1) of the GDPR.

“Supervisory Authority” means an independent public authority which is established by an EEA jurisdiction pursuant to Article 51 of the GDPR.

“Third Country” means any country that is not an EEA Member State.

“Vendor” means a corporate vendor of any In-Scope Nestlé Controller or In-Scope Nestlé Processor.

Appendix 2 – Data Flows

1 Categories of Data Subjects:

The categories of Data Subjects are as follows:

Category One	Nestlé Personnel
Category Two	Family members and other beneficiaries of Nestlé Personnel
Category Three	Job applicants
Category Four	Consumers, visitors to any Nestlé websites and visitors to Nestlé's premises
Category Five	Personnel of corporate Customers
Category Six	Personnel of corporate Vendors
Category Seven	Third parties (e.g., journalists with whom Nestlé interacts from time to time)
Category Eight	Participants in product development studies and clinical trials

2 Categories of Relevant Personal Data:

Subject always to the requirement that all transfers must be limited to the minimum necessary to achieve the lawful purposes of the relevant In-Scope Nestlé Affiliates, in accordance with the data minimisation principles set out in Clause 6 of these Controller BCRs, the categories of Relevant Personal Data that may be transferred under these Controller BCRs, the purposes of such transfers, and the Third Country destinations of such transfers, are as follows:

	Categories of affected Data Subjects	Category of Relevant Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
1)	Category One (Nestlé Personnel)	Name(s); preferred name(s); title/salutation; Nestlé employer entity; department; local position title; Personnel ID type and number; username; date of birth/age; nationality(ies); records of work-related correspondence; home address; work address; home telephone number; work telephone number; work mobile number; network ID; login details; biometric details (where relevant); work email address; employment percentage (full or part-time); original hire date; most recent hire date; service date; date of termination; company code (Personnel area); Personnel group/subgroup; organizational unit name; supervisor or manager name; job level; academic and vocational qualifications; vacations and vacation requests; usual work hours; languages spoken; experience; past employers; and past roles.	Business administration – Due to the global nature of Nestlé's business and the need for ease of internal communication and interaction among the human resources staff of the subsidiaries of Nestlé around the world, limited Personal Data of Nestlé Personnel needs to be transferred internationally under these Controller BCRs, as part of Nestlé's global internal contacts database, for the purpose of facilitating internal communication and interaction. The specific business administration purposes for which Relevant Personal Data in Category One may be transferred are: human resources management; internal communication; mobility management, including international assignment and Personnel travel; recruitment; advertising of positions; administration of Nestlé information technology systems; economic, financial and administrative management; business planning and reporting; Personnel development; attendance and absence management; performance management; appraisal/review; training/learning and personal development; accounting; finance; research and development (as further detailed in paragraph 7 of this Appendix 2); corporate audit; stock administration; emergency contacts; succession and organizational planning, including budgeting; governance and internal reporting; and work-related correspondence.	The Third Country(ies) (if any) in which the appropriate Nestlé managers and business administration teams are located, to the extent strictly necessary for the business administration purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
2)	Category One (Nestlé Personnel)	Name(s); preferred name(s); gender (if specified); photograph (if provided and if relevant); title/salutation; Nestlé employer entity; department; local position title; work address; work email address; work telephone number; work mobile number; Personnel group/subgroup; supervisor name; organizational unit name; and job level.	Nestlé Personnel databases – Due to the global nature of Nestlé's business and the need for ease of internal communication and interaction within the business, all Personnel with access to Nestlé's IT systems will have access to this information, as this is necessary for the day-to-day operation of Nestlé's global businesses.	All Nestlé In-Scope Affiliate locations.

	Categories of affected Data Subjects	Category of Relevant Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
3)	Category One (Nestlé Personnel)	Name(s); preferred name(s); title/salutation; Nestlé employer entity; department; local position title; payroll system ID; Personnel ID type and number; work address; work telephone number; work mobile number; work email address; CVs and covering letters; applications submitted; applications accepted (with reasons); applications rejected (with reasons); positions or roles applied for; languages spoken; experience; past employers; past roles; reference letters from past employers.	Recruitment – Operation and improvement of recruitment purposes.	The Third Country(ies) (if any) in which the appropriate Nestlé recruitment teams are located, to the extent strictly necessary for the recruitment purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
4)	Category One (Nestlé Personnel)	Name(s); preferred name(s); title/salutation; Nestlé employer entity; department; local position title; payroll system ID; Personnel ID type and number; work address; work telephone number; work mobile number; work email address; marital status (for tax and benefits purposes only); visa number; work authorization number; date of birth/age; nationality(ies); bank account information; tax code and number; work permit data; salary and benefits; hourly rate (where applicable); target commission; bonus type; stock awards; eligibility for bonus and/or long-term income; pension details; employment percentage (full or part-time); original hire date; most recent hire date; service date; company code (Personnel area); Personnel group/subgroup; organizational unit name; probation end date; job level; vacation dates; hours worked (where relevant to compensation or benefits); date of termination; work-related expenses (including travel expenses); and details of family members and other designated beneficiaries (see Category Two below in this table).	Compensation and benefits administration – Administration of payroll, compensation, incentives programs, benefits and pensions; expense reimbursement; compensation planning and payments; and tax planning and compliance.	The Third Country(ies) (if any) in which the appropriate Nestlé managers and finance teams are located, to the extent strictly necessary for the compensation and benefits administration purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.

	Categories of affected Data Subjects	Category of Relevant Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
5)	Category One (Nestlé Personnel)	Name(s); preferred name(s); photograph (if provided and if relevant); title/salutation; Nestlé employer entity; department; local position title; Personnel ID type and number; username; work address; work telephone number; work mobile number; network ID; login details; work email address; information concerning the use of, and Personal Data transmitted through, Nestlé information systems; and, for a limited number of Nestlé Personnel, work-related social media profiles (not including personal social media profiles or account details).	IT services and information security – Provision, maintenance, support and development of the Nestle IT systems; implementing, maintaining and improving information security systems and measures; developing and issuing IT-related policies and procedures; investigating IT security incidents and Personal Data Breaches; and monitoring of IT systems for threats (subject to compliance with applicable law).	The Third Country(ies) (if any) in which the appropriate Nestlé managers and IT teams are located, to the extent strictly necessary for the IT services and information security purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
6)	Category One (Nestlé Personnel)	Name(s); preferred name(s); gender (if specified); photograph (if provided and if relevant); title/salutation; work address; work telephone number; work mobile number; work email address; Nestlé employer entity; department; local position title; Personnel learning objectives; progress and results; academic and vocational qualifications; Personnel development plan; Personnel performance objectives and appraisal results; Personnel self-assessment results; training undertaken and completed; and dates of training scheduled and completed.	Personnel training and careers – Managing and facilitating Personnel training and career development and planning.	The Third Country(ies) (if any) in which the appropriate Nestlé managers are located, to the extent strictly necessary for the training and careers purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
7)	Category One (Nestlé Personnel)	Name(s); preferred name(s); gender (if specified); photograph (if provided and if relevant); title/salutation; work address; work telephone number; work mobile number; work email address; Nestlé employer entity; department; local position title; Personnel ID type and number; passport number; visa number; work authorization number; date of birth/age; nationality(ies); and work permit information.	Personnel mobility and travel – Managing and facilitating Personnel mobility, employment across jurisdictions, and travel.	The Third Country(ies) (if any) in which the appropriate Nestlé managers are located, to the extent strictly necessary for the mobility and travel purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.

	Categories of affected Data Subjects	Category of Relevant Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
8)	Category One (Nestlé Personnel)	Name(s); preferred name(s); gender (if specified); photograph (if provided and if relevant); title/salutation; work address; work telephone number; work mobile number; work email address; Nestlé employer entity; department; local position title; compliance information; training records; actual and alleged violations of Nestlé policies; reports of violations of internal policies and codes of conduct; disciplinary sanctions; manager's name and reporting structure; acknowledgments regarding internal policies; and date and reason for resignation or termination.	Internal compliance – Compliance with internal policies, codes of conduct and legal/regulatory compliance; disciplinary and grievance investigations; and disciplinary procedures.	The Third Country(ies) (if any) in which the appropriate Nestlé investigators and managers are located, to the extent strictly necessary for the investigations and disciplinary purposes specified in this row, and to establish, exercise or defend legal claims arising in relation to the same, subject always to compliance with applicable law.
9)	Category One (Nestlé Personnel)	Name(s); preferred name(s); gender (if specified); photograph (if provided and if relevant); title/salutation; work address; work telephone number; work mobile number; work email address; Nestlé employer entity; department; local position title; compliance information; training records; and evidence gathered in the course of the investigation, reports generated as part of the investigation and response taken by Nestlé's companies in the context of Nestlé's whistleblowing hotline (the "Hotline"); and facts reported through the Hotline.	Hotline operation – Implementation and operation of the Hotline; investigations into allegations or information reported via the Hotline; management workplace relations relating to Hotline reporting.	The Hotline is operated using servers in the EEA. Relevant Personal Data reported to the Hotline is kept within the jurisdiction to which the relevant report relates. Personal data reported to the Hotline in relation to an EEA Member State may be transferred out of the EEA to Switzerland only, and only to the extent strictly necessary for centralized reporting purposes.
10)	Category One (Nestlé Personnel)	Name(s); preferred name(s); gender (if specified); photograph (if provided and if relevant); title/salutation; work address; work telephone number; work mobile number; work email address; Nestlé employer entity; department; local position title; workplace health and safety records; details of any health or safety incidents in the workplace; work absence and attendance records related to health and safety incidents or issues; and emergency contact details	Workplace health and safety management – Implementation and operation of workplace health and safety measures; accident recording and reporting; and arranging medical care where necessary.	The Third Country(ies) (if any) in which the appropriate Nestlé managers and safety teams are located, to the extent strictly necessary for the workplace health and safety management purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.

	Categories of affected Data Subjects	Category of Relevant Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
11)	Category Two (Family members & beneficiaries of Nestlé Personnel)	Name(s); preferred name(s); residential address; date of birth/age; marital status; relationship to Nestlé Personnel; applicable benefits and pensions records; benefits and pensions claims; and records of correspondence.	Compensation and benefits administration – Administration of relevant incentives programs, benefits and pensions; and tax planning and compliance.	The Third Country(ies) (if any) in which the appropriate Nestlé finance, accounting, benefits and human resources teams are located, to the extent strictly necessary for the compensation and benefits administration purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
12)	Category Two (Family members & beneficiaries of Nestlé Personnel)	Name(s); preferred name(s); and emergency contact details.	Emergency contacts of Nestlé Personnel – Contacting the emergency contacts of the relevant Personnel when required in accordance with applicable Nestlé policies (e.g., in the event of a workplace accident or other emergency).	The Third Country(ies) (if any) in which the appropriate Nestlé managers and safety teams are located, to the extent strictly necessary for the emergency contact purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.

	Categories of affected Data Subjects	Category of Relevant Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
13)	Category Three (Job applicants)	Current and previous name(s); preferred name(s); current and previous title/salutation(s); current home address; previous home address(es); telephone number; mobile number; email address; academic and vocational qualifications; experience; languages spoken; date of birth/age; nationality(ies); passport number; visa number; work authorization number; work permit data; national insurance number; social security number; past employers; past roles; CVs and covering letters; applications submitted; reference letters from past employers and others; positions or roles applied for; Nestlé employer entity; department; position title; salary and benefits; hourly rate (where applicable); target commission; bonus type; stock awards; eligibility for bonus and/or long-term income; pension details; employment percentage (full or part-time); application date; interview date; date on which a decision was made about employment; applications accepted (with reasons); applications rejected (with reasons).	Recruitment – Operation and improvement of recruitment purposes; processing applications for employment with Nestlé; determining whether applicants will be suitable for positions within Nestlé; conducting background investigations and right to work checks; and reporting purposes.	The Third Country(ies) (if any) in which the appropriate Nestlé recruitment teams, Nestlé managers and business administration teams, and/or external recruiters and referees, are located, to the extent strictly necessary for the recruitment purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
14)	Category Four (Consumers and visitors)	Name(s); gender (if specified); photograph (if provided and if relevant); title/salutation; date of birth/age; contact information (including email address, postal address and telephone number); network security data (e.g., IP addresses, suspicious activity indicators, etc.); cookie data; interests; preferences; consumer questions and complaints; website login details; account details; payment details and credit/debit card information; delivery address; billing address; order details; purchase records; invoice records; digital shopping basket data; clickstream data; records of interactions with Nestlé websites; digital marketing; and records of marketing preferences.	Consumer relations – Management of Consumer relations; security, operation and management of Nestlé's websites; administration and operation of cookies in accordance with applicable laws; management of online Consumer accounts; provision of tailored services (including interests and preferences); handling of Consumer questions and complaints; facilitation of online shopping activities; research and development (as further detailed in paragraph 7 of this Appendix 2); management of digital shopping baskets; management of purchase records and receipts; provision and development of consumer-facing services; advertising and marketing; and recording and giving effect to marketing preferences in accordance with applicable laws.	The Third Country(ies) (if any) in which the appropriate Nestlé finance, accounting, Consumer relations, security and facilities management teams are located, to the extent strictly necessary for the consumer relations purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.

	Categories of affected Data Subjects	Category of Relevant Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
15)	Category Four (Consumers and visitors)	Visitor details; gender (if specified); photograph (if provided and if relevant); dates of visits to Nestlé facilities; travel plans and itineraries involving Nestlé; meeting schedules involving Nestlé; visitor logs and analogous records; building access records; security and operations records; and records of correspondence.	Visitor relations – Managing visitor attendance at Nestlé facilities; limiting access to authorised areas; facility security; and health and safety measures.	The Third Country(ies) (if any) in which the appropriate Nestlé managers and facilities teams are located, to the extent strictly necessary for the visitor relations purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
16)	Category Five (Personnel of corporate Customers)	Name(s); gender (if specified); photograph (if provided and if relevant); title/salutation; date of birth/age; contact information (including address and other contact information, such as work-related telephone numbers and email addresses); job title and role/function; individual contact details recorded in connection with Customer purchases and marketing activities.	Corporate Customer relations – Managing and administering relationships with corporate Customers; corporate Customer contract management and renewal; business administration; maintaining lists of contacts at Customers; making bids and proposals to Customers; sales; payment processing; business-to-business marketing, advertising and promotional activities; Customer support; Customer relationship management; research and development (as further detailed in paragraph 7 of this Appendix 2); budgeting and planning; business operations including management, processing and fulfilment of Customer orders; and recording and giving effect to marketing preferences in accordance with applicable laws.	The Third Country(ies) (if any) in which the appropriate Nestlé Customer relationship management, finance, accounting, sales, marketing, and management teams are located, to the extent strictly necessary for the corporate Customer relations purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.

	Categories of affected Data Subjects	Category of Relevant Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
17)	Category Six (Personnel of corporate Vendors)	Name(s); gender (if specified); photograph (if provided and if relevant); title/salutation; date of birth/age; contact information (including business address and other contact information such as personal telephone numbers and email addresses); job title and role/function; individual contact details recorded on Vendor task records, Vendor budgets, Vendor contracts, Vendor delivery dates and timelines, Vendor account/payment data; and records of correspondence.	Vendor relations – Managing and administering relationships with corporate Vendors; business administration; procurement; maintaining lists of contacts at Vendors; managing bids and proposals from Vendors; Vendor engagement; Vendor relationship management; Vendor services management; research and development (as further detailed in paragraph 7 of this Appendix 2); budgeting and planning; Vendor performance assessments; business operations including management and renewal of Vendor contracts and correspondence.	The Third Country(ies) (if any) in which the appropriate Nestlé Vendor relationship management, finance, accounting, and procurement teams are located, to the extent strictly necessary for the vendor relations purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
18)	Category Seven (Third parties)	Name(s); gender (if specified); photograph (if provided and if relevant); title/salutation; date of birth/age; contact information (including business address and other contact information such as personal telephone numbers and email addresses); job title and role/function; and records of correspondence.	External relations – Business administration and management; managing contact directories; press management; public relations; interactions with journalists; and correspondence.	The Third Country(ies) (if any) in which the appropriate Nestlé public relations and management teams are located, to the extent strictly necessary for the external relations purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
19)	Category Eight (Research participants)	Records of participation in research panels; records of completed research questionnaires; clinical trial data (key coded in accordance with applicable law and guidelines); nutrivigilance data; pharmacovigilance data; records of consents; records of notices; and records of correspondence.	Research and development – Conducting research panels; gathering feedback through research questionnaires; conducting clinical trials; nutrivigilance; pharmacovigilance; obtaining any necessary consents; providing required notices; and correspondence.	The Third Country(ies) (if any) in which the appropriate Nestlé research and development teams are located, to the extent strictly necessary for the research and development purposes specified in this row. In practice, the most common destination Third Country is the United States.

	Categories of affected Data Subjects	Category of Relevant Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
20)	All categories of Data Subjects listed above in this table.	All categories of Relevant Personal Data listed above in this table, to the extent strictly necessary for the purposes specified in this row.	Processing of Relevant Personal Data by Nestlé Processors in accordance with the instructions of the relevant In-Scope Nestlé Controller.	Personal data in all categories may be transferred to the Nestlé Processors listed in Paragraph 5 of this Appendix 2 (as amended from time to time) to the extent necessary to Process Relevant Personal Data in accordance with the instructions of the relevant In-Scope Nestlé Controller, subject always to compliance with the requirements of these Controller BCRs and, in particular, Clauses 1.1(b), 14.3 and 19.
21)	All categories of Data Subjects listed above in this table.	All categories of Relevant Personal Data listed above in this table, to the extent strictly necessary for the purposes specified in this row.	Detection, investigation and prevention of fraud and other unlawful activities.	The Third Country(ies) (if any) in which the appropriate Nestlé investigators and managers and/or authorities are located, to the extent strictly necessary for the investigation and prevention purposes specified in this row, and to establish, exercise or defend legal claims arising in relation to the same, subject always to compliance with applicable law.

3 Transfers of Sensitive Personal Data:

Subject to applicable law, the categories of Relevant Sensitive Personal Data that may be transferred and otherwise Processed under these Controller BCRs, the purposes of such transfers, and the Third Countries of destination for each such transfer are as follows:

	Categories of affected Data Subjects	Category of Relevant Sensitive Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
1)	Category One (Nestlé Personnel)	Health data (sick leave information, records of workplace injuries and industrial accidents)	• Maintaining records of sick leave and industrial accidents, in accordance with applicable employment law, and health & safety legislation. • Managing insurance claims in relation to employee absences.	The Third Country(ies) (if any) in which the appropriate Nestlé managers and health and safety teams are located, to the extent strictly necessary for the purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
2)	Category One (Nestlé Personnel)	Trade union membership	• Maintaining records of trade union membership, in accordance with applicable employment law.	The Third Country(ies) (if any) in which the appropriate Nestlé managers and human resources teams are located, to the extent strictly necessary for purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.

	Categories of affected Data Subjects	Category of Relevant Sensitive Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
3)	Category One (Nestlé Personnel)	Religion	• Managing employee relations in relation to religious requirements in accordance with applicable employment law (e.g., Personnel of particular religions may be unable to work on certain days, or may be unable to work with certain products). • Diversity and inclusion reporting and aggregated statistics.	The Third Country(ies) (if any) in which the appropriate Nestlé managers and human resources teams are located, to the extent strictly necessary for the purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
4)	Category One (Nestlé Personnel)	National ID documents[1]	• Managing employee relations in accordance with applicable employment law (e.g., handling Personnel visas and work permits).	The Third Country(ies) (if any) in which the appropriate Nestlé human resources and industrial relations teams are located, to the extent strictly necessary for purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.

[1] Although national ID documents are not treated as Sensitive Personal Data in the GDPR itself, such documents are treated as Sensitive Personal Data in some EU Member States, and are therefore considered Sensitive Personal Data for the purposes of these Controller BCRs.

	Categories of affected Data Subjects	Category of Relevant Sensitive Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
5)	Category One (Nestlé Personnel)	Biometric data (fingerprints)	• In a limited number of facilities, Nestlé uses biometric security measures, in accordance with applicable law, for security purposes and to guarantee limited access to restricted areas.	The Third Country(ies) (if any) in which the appropriate Nestlé facilities and IT security teams are located, to the extent strictly necessary for purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
6)	Category Four (Consumers)	Health data (consumer allergies)	• Responding to consumer queries; ensuring that Consumers are offered appropriate information regarding products to which they may be allergic. • Managing insurance claims in relation to complaints by Consumers.	The Third Country(ies) (if any) in which the appropriate Nestlé managers, consumer relations, and legal teams are located, to the extent strictly necessary for purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
7)	Category Four (Consumers)	Health data (pharmacovigilance data)	• In the event that a medicinal product causes an adverse health reaction, Nestlé may contact affected Consumers for pharmacovigilance purposes to alert them to any relevant health dangers, or for other necessary Consumer safety purposes including advice on proper product usage. • Managing insurance claims in relation to complaints by Consumers.	The Third Country(ies) (if any) in which the appropriate Nestlé pharmacovigilance, consumer relations, and legal teams are located, to the extent strictly necessary for purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.

	Categories of affected Data Subjects	Category of Relevant Sensitive Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
8)	Category Four (Consumers)	Health data (nutrivigilance data)	• In the event that a Nestlé food product causes an adverse health reaction, Nestlé may contact affected Consumers for nutrivigilance purposes to alert them to any relevant health dangers, or for other necessary Consumer safety purposes including advice on appropriate dietary restrictions. • Managing insurance claims in relation to complaints by Consumers.	The Third Country(ies) (if any) in which the appropriate Nestlé nutrivigilance, consumer relations, and legal teams are located, to the extent strictly necessary for purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
9)	Category Four (Consumers)	Religion	• Responding to consumer queries that relate to their religion (e.g., whether a given food product meets the requirements of their religion); and ensuring that Consumers are offered appropriate information regarding products compatible with their religious beliefs.	The Third Country(ies) (if any) in which the appropriate Nestlé managers and consumer relations teams are located, to the extent strictly necessary for purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
10)	Category Four (Consumers)	National ID documents	• In some cases, Data Subjects send their national ID documents to Nestlé (e.g., as evidence of identity in the context of exercising their rights under Chapter III of the GDPR).[2] Nestlé processes that information to the extent necessary to give effect to the rights of the Data Subject, and thereafter promptly deletes the national ID document data, in accordance with the Nestlé Record Retention Rules.	The Third Country(ies) (if any) in which the appropriate Nestlé managers, human resources, and legal teams are located, to the extent strictly necessary for purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.

[2] Nestlé does not request such information unless it is appropriate to do so in accordance with Article 12(6) of the GDPR. Nevertheless, some Data Subjects send copies of their ID documents without being asked to do so (e.g., when making requests to exercise their rights under Chapter III of the GDPR).

	Categories of affected Data Subjects	Category of Relevant Sensitive Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
11)	Category Eight (Research participants)	Health data (product testing data)	• Data Subjects may voluntarily choose to participate in research and development projects (e.g., testing of new food products or healthcare products). Nestlé processes that information to the extent necessary to complete the testing, and thereafter promptly deletes the relevant health data, in accordance with the Nestlé Record Retention Rules.	The Third Country(ies) (if any) in which the appropriate Nestlé managers, research and development, and legal teams are located, to the extent strictly necessary for purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
12)	Category Eight (Research participants)	Health data (pharmacovigilance data)	• In the event that a medicinal product causes an adverse health reaction, Nestlé may contact affected research participants for pharmacovigilance purposes to alert them to any relevant health dangers, or for other necessary consumer safety purposes including advice on proper product usage.	The Third Country(ies) (if any) in which the appropriate Nestlé pharmacovigilance, research and development, and legal teams are located, to the extent strictly necessary for purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.

	Categories of affected Data Subjects	Category of Relevant Sensitive Personal Data transferred	Purposes of Processing	Third Country(ies) of destination
13)	Category Eight (Research participants)	Health data (nutrivigilance data)	• In the event that a Nestlé food product causes an adverse health reaction, Nestlé may contact affected research participants for nutrivigilance purposes to alert them to any relevant health dangers, or for other necessary Consumer safety purposes including advice on appropriate dietary restrictions.	The Third Country(ies) (if any) in which the appropriate Nestlé nutrivigilance, research and development, and legal teams are located, to the extent strictly necessary for purposes specified in this row. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.
14)	All categories of Data Subjects listed above in this table.	All categories of Relevant Personal Data listed above in this table, to the extent strictly necessary for the purposes specified in this row.	• Detection, investigation and prevention of fraud and other unlawful activities.	The Third Country(ies) (if any) in which the appropriate Nestlé investigators and managers and/or authorities are located, to the extent strictly necessary for the investigation and prevention purposes specified in this row, and to establish, exercise or defend legal claims arising in relation to the same, subject always to compliance with applicable law. In practice, the most common destination Third Countries are Switzerland, Ukraine, Brazil and the Philippines.

4 Data protection registration information of Data Exporters:

The Data Exporters have registered and/or will register their data Processing operations as required by law.

5 List of existing Nestlé Processors:

- Globe Center Europe GmbH for EUR Markets, Lyoner Strasse 23, 60528, Frankfurt am Main, Germany;
- Société des Produits Nestlé S.A (SPN) (previously Nestec SA) for GCEUR and EUR Markets, Avenue Nestlé 55, 1800, VEVEY, Switzerland;
- Nestlé Operating Services Worldwide ("NOSW") for GCEUR and EUR Markets, Route de Buyère 4, 1030, BUSSIGNY-PRES-LAUSANNE, Switzerland;
- NBS LVIV for NOSW as a subcontractor Uhorska st. 14 79034 Lviv Ukraine;
- NBS Centre Lviv for EUR Markets Uhorska st. 14 79034 Lviv Ukraine;
- NBS Ribeirao Preto for SPN 300 Henri Nestle Ave, Ribeiro Preto-SP, 14094-000,Brazil;
- NBS Malaysia for Nestec and EUR Markets Supima E-Circle Mahalcan Road, Meycauayan City, Bulacan, Philippines; and
- Nestrade for GCEUR ad EUR Markets, Avenue Reller 22, 1800, Vevey, Switzerland.

6 Data Privacy eLearning for Nestlé Personnel

Nestlé has developed interactive, relevant, engaging, up-to-date and regularly refreshed training for all Nestlé Personnel who Process Relevant Personal Data as part of their assigned duties. The training addresses compliance with obligations applicable to such Personnel under data protection laws in general, and these Controller BCRs in particular. Nestlé's Personnel data protection training program is designed to provide such Nestlé Personnel with the skills, knowledge, resources and practice opportunities they require in order to help ensure that Relevant Personal Data is Processed in accordance with these Controller BCRs.

The training is subdivided in four key topics as follows:

(i) "Why is privacy important?";
(ii) "What is personal data?";
(iii) "How should I handle personal data?"; and
(iv) "What can I share?".

Training participants are asked a number of interactive multiple choice questions during the training, and are provided with feedback on their responses. For example, they are asked to indicate in a list the possible consequences of a Personal Data Breach or to identify what constitutes Personal Data and what does not. The training focuses on real-life situations and uses plain language to ensure all categories of Personnel are able to follow it.

The training completion is logged and verified for all employees, with the aim to achieve the training of 100% of the employees with assigned company computers on this basis.

7 Research and development

As noted above in this Appendix 2, Relevant Personal Data may be Processed for research and development purposes, which are further detailed in the table below. In practice, the most common destination Third Country for such transfers is the United States.

	Category of Relevant Personal Data	Categories of affected Data Subjects	Purposes of Processing
1)	Name(s); contact information; demographics; interests; records of participation in research panels; records of consents provided by the data subjects (e.g. to participate in testing or to receive information / sign-up for newsletters or to be part of a panel for future projects); records of completed research questionnaires and other information provided by the Consumers / participants directly or indirectly within the scope of the research; records of correspondence; and payment and financial information.	Category Eight (Research Participants); Category Four (Consumers)	• Relevant Personal Data of research participants, or Consumers who have agreed to provide feedback to Nestlé, are Processed for the purpose of researching product design, and product development and/or improvements, through soliciting product, taste or experience feedback, engaging Consumers through research panels online and face-to-face, and asking Consumers to complete research questionnaires or otherwise provide information.

	Category of Relevant Personal Data	Categories of affected Data Subjects	Purposes of Processing
2)	Name(s); contact information; records of participation in research panels; records of completed research questionnaires; and records of correspondence.	Category Five (Personnel of corporate Customers)	• Relevant Personal Data of Personnel of corporate customers and business collaborators are Processed for the purposes of researching product improvements, through soliciting product feedback, engaging representatives of corporate Customers and business collaborators through research panels, and asking Personnel of corporate Customers or business collaborators to complete research questionnaires.
3)	Name(s); gender; ethnicity; title/salutation; date of birth/age; contact information; records of participation in research projects (e.g. clinical trials, observational studies); pharmacovigilance data where required; (serious) adverse event related data; demographics; clinical trial data including health related data as defined under the protocol of each project (key coded in accordance with applicable law and guidelines); records of consents provided by the data subjects; and records of correspondence.	Category Eight (Research Participants)	• Relevant data from participants in Nestlé sponsored clinical trials, studies, or other research projects, databases or biobanks, or of such projects sponsored by a Nestlé collaborator / third party (e.g., a database licensed to Nestlé), for the purposes of: (1) designing, implementing and conducting the research project or method development/validation, (2) compliance with any applicable legal, medical, or ethical obligations (e.g., pharmacovigilance), and (3) archiving as required or permitted under applicable law. • To the extent permitted by applicable law, and in accordance with the information provided to the Data Subjects at the time of collection of the Personal Data, such Personal Data may be further used for other research projects (secondary use) (and/or further data may be derived from stored biological samples).

	Category of Relevant Personal Data	Categories of affected Data Subjects	Purposes of Processing
4)	Name(s); title/salutation; employer details; records of participation in research projects (e.g. clinical trials, observational studies); pharmacovigilance data where required (e.g., in connection with potential exposure of such Personnel to health risks); qualifications of the principal investigator and other personnel involved (e.g., titles, CVs, required certifications); performance considerations; records of consents provided by the data subjects; and records of correspondence.	Category Six (Personnel at the vendors / hospitals / sites involved in research projects)	• Personal data of Personnel at the vendors / hospitals / sites involved in the projects may be Processed for the purposes of ensuring the accuracy of study data, following up on incomplete questionnaires, and checking statistical anomalies (e.g., over-performance or under-performance in gathering completed questionnaires). Such data is Processed solely for the purpose of ensuring the accuracy and completeness of the relevant research, or to the extent necessary for compliance with any applicable legal, medical, or ethical obligations (e.g., pharmacovigilance).

Appendix 3 – Internal Complaints Handling Procedure

1 Defined terms

1.1 Except where expressly stated otherwise, capitalised terms used in this Procedure have the meanings given in the Nestlé Controller BCRs.

1.2 The Group Data Protection Officer is appointed by Nestlé S.A., and acts on behalf of Nestlé France under power of attorney. The Group Data Protection Officer is tasked with overseeing data protection compliance by Nestlé Affiliates. All references to the "Group Data Protection Officer" include the members of the Group Data Protection Office.

2 Publication

2.1 This Procedure is internal to Nestlé, but the features of this Procedure that are applicable to Data Subjects will be included in Nestlé's public-facing privacy notices issued in respect of the Nestlé Controller BCRs.

3 Scope

3.1 Any Data Subject who believes that an In-Scope Nestlé Controller has failed to comply with the requirements of the Nestlé Controller BCRs may make a complaint in accordance with the provisions of this Procedure.

3.2 Where an In-Scope Nestlé Processor receives any correspondence (including any complaint) in connection with the Nestlé Controller BCRs, in its capacity as a Processor, from a Data Subject, that In-Scope Nestlé Processor will forward the correspondence to the relevant In-Scope Nestlé Controller(s) who will determine the appropriate response to the correspondence. Where a complaint regarding any aspect of the Nestlé Controller BCRs is received, that complaint will be handled in accordance with the complaints procedure below.

4 Making a complaint

4.1 Data Subjects may make a complaint by contacting, at the Data Subject's discretion:

(a) the local In-Scope Nestlé Controller using its published contact details in the applicable local privacy notice, which provides contact details for the relevant local Data Protection Champion; or

(b) the contact details provided by Nestlé at https://www.nestle.com/bcr; or

(c) the Group Data Protection Officer, either:

(i) by postal mail to: Nestlé S.A., Data Protection Officer, Avenue Nestlé 55, 1800 Vevey, Switzerland; or

(ii) by email to: dataprotectionoffice@nestle.com

4.2 There is no set format in which a complaint must be made. However, if the complaint is made electronically (e.g., via email) then the In-Scope Nestlé Controller, or the Group Data Protection Officer, as appropriate, will respond in the same format.

4.3 The relevant Nestlé privacy notice should explain that, when making a complaint, Data Subjects are encouraged to provide as much detail as possible about the facts giving rise to the complaint, including:

(a) the name and contact details of the Data Subject;

(b) the identities of the In-Scope Nestlé Controller(s) to whom the complaint relates (or, if that is not known, the Market to which the complaint relates);

(c) the provisions of the Nestlé Controller BCRs that are believed to have been infringed, or the issue in respect of which redress is requested, together with any documents or evidence of that infringement or issue; and

(d) any additional information that the Data Subject considers relevant or helpful to the complaint.

5 Immediate response to a complaint

Where the complaint is addressed to a local In-Scope Nestlé Controller, that Controller will review and respond to the complaint diligently by acknowledging receipt of the communication from the Data Subject, investigating the complaint, and responding to the Data Subject (including, where applicable, in accordance with the time limits set out in Article 12(3) of the GDPR, as set out in Appendix 4).

6 Evidence of the identity of the Data Subject

Where the relevant In-Scope Nestlé Controller(s) have reasonable doubts concerning the identity of the Data Subject making the request, the relevant In-Scope Nestlé Controller(s) may request the provision of additional information necessary to confirm the identity of the Data Subject.

7 Escalation of a complaint by Nestlé

Where a complaint is made to an In-Scope Nestlé Controller, the relevant local Data Protection Champion may, if necessary and appropriate, escalate the matter to the Group Data Protection Officer.

8 Investigation of complaints

8.1 Subject to Clause 8.2, the In-Scope Nestlé Controller, or the Group Data Protection Officer, as appropriate, will investigate the complaint and respond to a complaint without undue delay and, in any event, within one month of the date on which the complaint (and any necessary evidence of the Data Subject's identity) is received.

8.2 The period for responding to a complaint may be extended by two further months where necessary, taking into account the complexity and number of complaints received. The In-

Scope Nestlé Controller, or the Group Data Protection Officer, as appropriate, will inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

9 Resolving complaints

If the complaint is upheld, the In-Scope Nestlé Controller, or the Group Data Protection Officer, as appropriate, will implement (or procure the implementation of) appropriate remedial measures, to the extent necessary to:

(a) resolve the complaint;

(b) ensure compliance with the Nestlé Controller BCRs; and

(c) avoid any recurrence of the facts giving rise to the complaint.

10 Escalation of a complaint by the Data Subject

10.1 If the complaint is rejected, or if the Data Subject is not satisfied with the response from the In-Scope Nestlé Controller (where applicable) the Data Subject may contact the Group Data Protection Officer using the contact details set out above. The Group Data Protection Officer will use all reasonable endeavours to resolve the complaint, in accordance with this procedure.

10.2 In addition to the right of Data Subjects to lodge a complaint with the relevant In-Scope Nestlé Controller(s) or the Group Data Protection Officer, Data Subjects may also lodge a complaint with the competent Supervisory Authority or bring a claim before any court of competent jurisdiction as set out in Clause 26.2 of the Nestlé Controller BCRs.

Appendix 4 – Articles 12, 13 & 14 of the GDPR

This Appendix 4 sets out the text of Articles 12, 13 and 14 of the GDPR. Certain defined terms have been amended to match the definitions used in these Controller BCRs, but otherwise the text is unchanged. Please note that references to "Articles" in this Appendix 4 are references to Articles of the GDPR.

Article 12 of the GDPR

Transparent information, communication and modalities for the exercise of the rights of the Data Subject

1 The In-Scope Nestlé Controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to Processing to the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the Data Subject, the information may be provided orally, provided that the identity of the Data Subject is proven by other means.

2 The In-Scope Nestlé Controller shall facilitate the exercise of Data Subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the In-Scope Nestlé Controller shall not refuse to act on the request of the Data Subject for exercising his or her rights under Articles 15 to 22, unless the In-Scope Nestlé Controller demonstrates that it is not in a position to identify the Data Subject.

3 The In-Scope Nestlé Controller shall provide information on action taken on a request under Articles 15 to 22 to the Data Subject without undue delay and in any event 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. The In-Scope Nestlé Controller shall inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the Data Subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the Data Subject.

4 If the In-Scope Nestlé Controller does not take action on the request of the Data Subject, the In-Scope Nestlé Controller shall inform the Data Subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a Supervisory Authority and seeking a judicial remedy.

5 Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests

from a Data Subject are manifestly unfounded or excessive, in particular because of their repetitive character, the In-Scope Nestlé Controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request. The In-Scope Nestlé Controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6 Without prejudice to Article 11, where the In-Scope Nestlé Controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the In-Scope Nestlé Controller may request the provision of additional information necessary to confirm the identity of the Data Subject.

7 The information to be provided to Data Subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended Processing. Where the icons are presented electronically they shall be machine-readable.

8 The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Article 13 of the GDPR

Information to be provided where Relevant Personal Data are collected from the Data Subject

1 Where Relevant Personal Data relating to a Data Subject are collected from the Data Subject, the In-Scope Nestlé Controller shall, at the time when Relevant Personal Data are obtained, provide the Data Subject with all of the following information:

(a) the identity and the contact details of the In-Scope Nestlé Controller and, where applicable, of the In-Scope Nestlé Controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the Processing for which the Relevant Personal Data are intended as well as the legal basis for the processing;

(d) where the Processing is based on point (f) of Article 6(1), the legitimate interests pursued by the In-Scope Nestlé Controller or by a third party;

(e) the recipients or categories of recipients of the Relevant Personal Data, if any;

(f) where applicable, the fact that the In-Scope Nestlé Controller intends to transfer Relevant Personal Data to a Third Country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1),

reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2 In addition to the information referred to in paragraph 1, the In-Scope Nestlé Controller shall, at the time when Relevant Personal Data are obtained, provide the Data Subject with the following further information necessary to ensure fair and transparent Processing:

(a) the period for which the Relevant Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the In-Scope Nestlé Controller access to and rectification or erasure of Relevant Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability;

(c) where the Processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of Relevant Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Relevant Personal Data and of the possible consequences of failure to provide such data; and

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

3 Where the In-Scope Nestlé Controller intends to further Process the Relevant Personal Data for a purpose other than that for which the Relevant Personal Data were collected, the In-Scope Nestlé Controller shall provide the Data Subject prior to that further Processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4 Paragraphs 1, 2 and 3 shall not apply where and insofar as the Data Subject already has the information.

Article 14 of the GDPR

Information to be provided where Relevant Personal Data have not been obtained from the Data Subject

1 Where Relevant Personal Data have not been obtained from the Data Subject, the In-Scope Nestlé Controller shall provide the Data Subject with the following information:

(a) the identity and the contact details of the In-Scope Nestlé Controller and, where applicable, of the In-Scope Nestlé Controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the Processing for which the Relevant Personal Data are intended as well as the legal basis for the Processing;

(d) the categories of Relevant Personal Data concerned;

(e) the recipients or categories of recipients of the Relevant Personal Data, if any; and

(f) where applicable, that the In-Scope Nestlé Controller intends to transfer Relevant Personal Data to a recipient in a Third Country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2 In addition to the information referred to in paragraph 1, the In-Scope Nestlé Controller shall provide the Data Subject with the following information necessary to ensure fair and transparent Processing in respect of the Data Subject:

(a) the period for which the Relevant Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the Processing is based on point (f) of Article 6(1), the Legitimate Interests pursued by the In-Scope Nestlé Controller or by a third party;

(c) the existence of the right to request from the In-Scope Nestlé Controller access to and rectification or erasure of Relevant Personal Data or restriction of Processing concerning the Data Subject and to object to Processing as well as the right to data portability;

(d) where Processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the Relevant Personal Data originate, and if applicable, whether it came from publicly accessible sources; and

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

3 The In-Scope Nestlé Controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the Relevant Personal Data, but at the latest within one month, having regard to the specific circumstances in which the Relevant Personal Data are Processed;

(b) if the Relevant Personal Data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the Relevant Personal Data are first disclosed.

4 Where the In-Scope Nestlé Controller intends to further Process the Relevant Personal Data for a purpose other than that for which the Relevant Personal Data were obtained, the In-Scope Nestlé Controller shall provide the Data Subject prior to that further Processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5 Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the Data Subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that Processing. In such cases the In-Scope Nestlé Controller shall take appropriate measures to protect the Data Subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the In-Scope Nestlé Controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests; or

(d) where the Relevant Personal Data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Appendix 5 – Supplementary Measures

In-Scope Nestlé Affiliates will ensure that Relevant Personal Data is Processed in accordance with the following requirements:

1. The provisions of the Nestlé Security Requirements for Relevant Personal Data shall apply, appropriate to the risk associated with the relevant Processing.
2. In addition to the provisions of the Nestlé Security Requirements for Relevant Personal Data, each In-Scope Nestlé Affiliate shall, in relation to any Relevant Personal Data shall:

    (a) document and record requests for access received from public authorities, as well as the response provided, the legal reasoning and the actors involved, and provide such documentation to the Coordinating Party upon written request;

    (b) in the event that it receives any order or legal requirement to disclose Relevant Personal Data (an "Order"):

        (i) review the legality of, and challenge (including via interim measures) such Order if it concludes that there are grounds to do so, document the steps taken to analyse and challenge the Order, and provide such documentation to the Coordinating Party upon written request; and

        (ii) to inform the requesting public authority of the incompatibility of the order with the safeguards contained in these Controller BCRs, document the steps taken to notify that public authority, and provide such documentation to the Coordinating Party upon written request;

    and

    (c) in an appropriate and timely manner involve, and provide access to information to, the local Data Protection Officer (or, upon written request, to the Group Data Protection Office) and to Nestlé's legal and internal auditing services, on matters relating to the transfer of Relevant Personal Data under these Controller BCRs.