

**Procter & Gamble Exhibit B**  
**STANDARD CONTRACTUAL CLAUSES (Controllers – Module One)**

For the transfer of personal data to controllers established in third countries which do not ensure an adequate level of data protection.

**Name of the data exporting organization:** The Procter & Gamble Company  
**Address:** One Procter & Gamble Plaza, Cincinnati, Ohio 45202, United States of America,

On its own right and on behalf of its affiliates and subsidiaries in the EU, as listed in Annex I A/Schedule 1.

(“the data **exporter**”)

and

**Name of the data importing organization:**

**Address:**

**[Include if relevant:]** [on its own right and on behalf of its affiliates and subsidiaries, as listed in Schedule 2.]

(“the data **importer**”)

each a “Party”, together “the Parties”,

SECTION I

*Clause 1*

**Purpose and scope**

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)<sup>1</sup> for the transfer of personal data to a third country.
- (b) The Parties:
- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A (hereinafter each ‘data exporter’), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly

<sup>1</sup> Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915

or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

#### *Clause 2*

#### **Effect and invariability of the Clauses**

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

#### *Clause 3*

#### **Third-party beneficiaries**

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7
  - (ii) Clause 8 – Clause 8.5 (e) and Clause 8.9(b);
  - (iii) Clause 12 – Clause 12(a) and (d);
  - (iv) Clause 13;4
  - (v) Clause 15.1(c), (d) and (e);
  - (vi) Clause 16(e);
  - (vii) Clause 18 – Clause 18(a) and (b);
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

#### *Clause 4*

#### **Interpretation**

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*  
**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6*  
**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

*Clause 7 – Optional*  
**Docking clause**

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

*Clause 8*  
**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**8.1 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.

B. It may only process the personal data for another purpose:

- (i) where it has obtained the data subject's prior consent;
- (ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

- (iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

## 8.2 Transparency

- (a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
  - (i) of its identity and contact details;
  - (ii) of the categories of personal data processed;
  - (iii) of the right to obtain a copy of these Clauses;
  - (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
- (b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
- (c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
- (d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

## 8.3 Accuracy and data minimisation

- (a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
- (b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
- (c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

## 8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation<sup>2</sup> of the data and all back-ups at the end of the retention period.

---

<sup>2</sup> This requires rendering the data anonymous in such a way that the individual is no longer

## 8.5 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- (b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
- (e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
- (f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
- (g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

---

identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

## 8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

## 8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union<sup>3</sup> (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- (i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- (iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- (iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- (v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- (vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

## 8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

---

<sup>3</sup> The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

## 8.9 Documentation and compliance

- (a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- (b) The data importer shall make such documentation available to the competent supervisory authority on request.

### *Clause 9*

#### **Use of sub-processors**

*(intentionally omitted for Module 1—controller-to-controller transfers)*

### *Clause 10*

#### **Data subject rights**

- (a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. <sup>(10)</sup> The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
- (b) In particular, upon request by the data subject the data importer shall, free of charge:
  - (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
  - (ii) rectify inaccurate or incomplete data concerning the data subject;
  - (iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
- (c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
- (d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lay down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

- (i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
  - (ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
- (e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
- (f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
- (g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

*Clause*

11

**Redress**

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body<sup>4</sup> (3) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
- (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation

---

<sup>4</sup> The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.



(EU) 2016/679.

- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*

**Liability**

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- (c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

*Clause 13*

**Supervision**

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC  
AUTHORITIES

**Local laws and practices affecting compliance with the Clauses**

*Clause 14*

- (a) Local laws and practices affecting compliance with the Clauses The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable

to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. 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 Clauses.

- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) 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<sup>5</sup>;
  - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), 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 paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures

---

<sup>5</sup> As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The 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 data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

### *Clause 15*

## **Obligations of the data importer in case of access by public authorities**

### **15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the 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.

Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

- (c) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (d) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

### **15.2 Review of legality and data minimisation**

- (a) The data importer agrees to review the legality of the request for disclosure, 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 country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the 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 personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

- (b) The 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 country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The 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.

#### SECTION IV – FINAL PROVISIONS

##### *Clause 16*

##### **Non-compliance with the Clauses and termination**

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of

local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17*

**Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the data exporter, as specified in Annex I A. and Schedule 1

*Clause 18*

**Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of the EU Member State where the data exporter is established, as specified in Annex I A. and Schedule 1
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

—

ANNEX I

By signing we also agree to be bound by the Swiss and UK Addenda to the EU Commission Standard Contractual Clauses at Annexes III and IV.

A. LIST OF PARTIES

MODULE ONE: TRANSFER CONTROLLER to CONTROLLER

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Name: The Procter & Gamble Company

Address: One Procter & Gamble Plaza, Cincinnati, Ohio 45202, United States of America.

Contact person's name, position, and contact details:

Curtis Scribner
Global Data Protection Officer
Global Privacy/Cybersecurity Law
Ethics & Compliance Office
The Procter & Gamble Company
phone: 513.983.8655 • email: scribner.c@pg.com

Activities relevant to the data transferred under these Clauses: [Describe the purpose of the transfer e.g. Provision by the Importer of the services described in Schedule X of the Master Services Agreement]

By:

Signature and date:

Role: Controller

On behalf of its affiliates and subsidiaries in the EU, as specified in Schedule 1.

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Name: .....

Address: .....

Contact person's name, position and contact details: .....

Activities relevant to the data transferred under these Clauses: [Describe the purpose of the transfer e.g. Provision by the Importer of the services described in Schedule X of the Master Services Agreement]

Signature and date: .....

Role: Controller

2. ....

**B. DESCRIPTION OF TRANSFER**

The Parties agree that in addition to the details of the processing reflected below, the data importer may process personal data for the purposes detailed in data exporter’s third-party risk management system (“ARAVO”) which includes specific details of the engagements and services provided by data importer. Any details of the processing not provided in Annex 1 but reflected in ARAVO are also incorporated into this Annex 1 by reference.

*Categories of data subjects whose personal data is transferred*

**[Insert]**.....

*Categories of personal data transferred*

**[Insert]**.....

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

**[Insert]**.....

.....

- The safeguards applied for the transfer of sensitive data are set forth in Annex II .

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

**[Insert]**.....

*.Nature of the processing*

**[Insert]**.....

*Purpose(s) of the data transfer and further processing*

**[Insert]**.....

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

**[Insert]**.....

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

**[Insert]**.....

**COMPETENT SUPERVISORY AUTHORITY** *Identify the competent supervisory authority/ies in accordance with Clause 13*

To the extent that the data transfer is governed by the GDPR, the supervisory authority of the EU Member State where the data exporter is established, as specified in Annex I. A and Schedule 1. To the extent that the data transfer is governed by the Swiss Federal Act on Data Protection, the Swiss FDPIC.

## ANNEX II

**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL  
AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE  
DATA**

## EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

***[Insert description of Vendor's data security measures. The following list of security measures may be used as a model, but must be customized to Vendor's practices.]***

<p><b><i>Measures of pseudonymisation and encryption of personal data</i></b></p>	<ul style="list-style-type: none"> <li>• Pseudonymization, where possible;</li> <li>• Encryption at rest and encryption in transit;</li> <li>• Encryption key kept in the EU or with a trusted third party;</li> <li>• Limited timespan for using personal data “in the clear” (<u>i.e.</u>, in identifiable form);</li> <li>• <b>[Other: Vendor to complete]</b></li> </ul>
<p><b><i>Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services</i></b></p>	<ul style="list-style-type: none"> <li>• Confidentiality arrangements;</li> <li>• Information security policies and procedures;</li> <li>• Backup procedures;</li> <li>• Remote storage;</li> <li>• Mirroring of hard disks (<u>e.g.</u>, RAID technology);</li> <li>• Uninterruptible power supply;</li> <li>• Anti-virus/firewall protection, security patch management;</li> <li>• Intrusion prevention, monitoring and detection;</li> <li>• Availability controls to protect personal data against accidental destruction or loss;</li> <li>• <b>[Other: Vendor to complete]</b></li> </ul>
<p><b><i>Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident</i></b></p>	<ul style="list-style-type: none"> <li>• Business continuity plan;</li> <li>• Disaster recovery procedure;</li> <li>• Incident response plan;</li> <li>• <b>[Other: Vendor to complete]</b></li> </ul>
<p><b><i>Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational</i></b></p>	<ul style="list-style-type: none"> <li>• Internal and external audit program, audit reports and documentation;</li> <li>• Testing of back up processes and business continuity procedures;</li> <li>• Risk evaluation and system monitoring on a regular basis;</li> </ul>



<i>measures in order to ensure the security of the processing</i>	<ul style="list-style-type: none"> <li>• Vulnerability and penetration testing on a regular basis;</li> <li>• <b>[Other: Vendor to complete]</b></li> </ul>
<i>Measures for user identification and authorisation</i>	<ul style="list-style-type: none"> <li>• Internal policies and procedures;</li> <li>• User authentication controls, including secure methods of assigning selecting and storing access credentials and blocking access after a reasonable number of failed authentication access;</li> <li>• Restricting access to certain users;</li> <li>• Access granted based on a need-to-know, supported by protocols for access authorization, establishment, modification and termination of access rights;</li> <li>• Logging and reporting systems;</li> <li>• Control authorization schemes;</li> <li>• Differentiated access rights (profiles, roles, transactions and objects);</li> <li>• Monitoring and logging of accesses;</li> <li>• Disciplinary action against employees who access personal data without authorization;</li> <li>• Reports of access;</li> <li>• Access procedure;</li> <li>• Change procedure;</li> <li>• <b>[Other: Vendor to complete]</b></li> </ul>
<i>Measures for the protection of data during transmission</i>	<ul style="list-style-type: none"> <li>• Encryption in transit;</li> <li>• Pseudonymization, where possible;</li> <li>• Transport security;</li> <li>• Network segregation;</li> <li>• Logging;</li> <li>• Electronic signatures;</li> <li>• <b>[Other: Vendor to complete]</b></li> </ul>
<i>Measures for the protection of data during storage</i>	<ul style="list-style-type: none"> <li>• Encryption at rest;</li> <li>• Access controls;</li> <li>• Separation of databases and logical segmentation of P&amp;G personal data from data of other vendor customers;</li> <li>• “Internal client” concept / limitation of use;</li> <li>• Segregation of functions (production/testing);</li> <li>• Procedures for storage, amendment, deletion, transmission of data for different purposes;</li> <li>• Process Personal Data in multiple separate locations or by using multiple parties;</li> <li>• <b>[Other: Vendor to complete]</b></li> </ul>
<i>Measures for ensuring physical security of locations at which personal data are processed</i>	<ul style="list-style-type: none"> <li>• Establishing security areas, restriction of access paths;</li> <li>• Establishing access authorizations for employees and third parties with a need-to-know;</li> </ul>

	<ul style="list-style-type: none"> <li>• Access control system (ID reader, magnetic card, chip card);</li> <li>• Key management, card-keys procedures;</li> <li>• Door locking (electric door openers etc.);</li> <li>• Security staff, janitors;</li> <li>• Surveillance facilities, video/CCTV monitor, alarm system;</li> <li>• Securing decentralized processing equipment and personal computers;</li> <li>• <b>[Other: Vendor to complete]</b></li> </ul>
<i>Measures for ensuring events logging</i>	<ul style="list-style-type: none"> <li>• User identification and authentication procedures;</li> <li>• ID/password security procedures (special characters, minimum length, change of password);</li> <li>• Automatic blocking (e.g., password or timeout);</li> <li>• Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;</li> <li>• Creation of one master record per user;</li> <li>• Encryption and pseudonymization;</li> <li>• <b>[Other: Vendor to complete]</b></li> </ul>
<i>Measures for ensuring system configuration, including default configuration</i>	<ul style="list-style-type: none"> <li>• Up-to-date baseline configuration documentation and settings;</li> <li>• <b>[Other: Vendor to complete]</b></li> </ul>
<i>Measures for internal IT and IT security governance and management</i>	<ul style="list-style-type: none"> <li>• Information security policies and procedures;</li> <li>• Incident response plan;</li> <li>• Regular internal and external audit;</li> <li>• Review and supervision of information security program;</li> <li>• <b>[Other: Vendor to complete]</b></li> </ul>
<i>Measures for certification/assurance of processes and products</i>	<p><b>[Vendor to confirm/complete as appropriate:]</b></p> <ul style="list-style-type: none"> <li>• [ISO27001, ISO27002, ISO27017, ISO27018, ISO 27701]</li> <li>• [NIST SP800-53, NIST CSF]</li> <li>• [SOC II]</li> <li>• [PCI DSS]</li> <li>• <b>[Other International standards and frameworks: Vendor to complete]</b></li> </ul>
<i>Measures for ensuring data minimisation</i>	<ul style="list-style-type: none"> <li>• Documentation regarding which data categories need to be processed;</li> <li>• Ensure that the minimum amount of data is processed to fulfill the purpose of the processing;</li> <li>• Personal data is stored in the EU and only remote access or view-only access is enabled;</li> </ul>
<i>Measures for ensuring data quality</i>	<ul style="list-style-type: none"> <li>• Personal data is kept accurate and up to date;</li> </ul>

	<ul style="list-style-type: none"> <li>• Data is corrected upon request or where necessary;</li> </ul>
<i>Measures for ensuring limited data retention</i>	<ul style="list-style-type: none"> <li>• Records retention schedule;</li> <li>• Data retention policy;</li> <li>• Personal data is deleted or irreversibly anonymized after expiration of the retention period;</li> </ul>
<i>Measures for ensuring accountability</i>	<ul style="list-style-type: none"> <li>• Internal policies and procedures;</li> <li>• Privacy by design and by default;</li> <li>• Records of data processing activities;</li> <li>• Privacy Impact Assessments, where required;</li> <li>• Adequate agreements with third parties;</li> <li>• Criteria for selecting the sub-processors;</li> <li>• Vendor onboarding process and questionnaire;</li> <li>• Monitoring of contract performance;</li> <li>• GDPR and InfoSec training program;</li> <li>• <b>[Other: Vendor to complete]</b></li> </ul>
<i>Measures for allowing data portability and ensuring erasure</i>	<ul style="list-style-type: none"> <li>• Personal data is made available upon request in an electronically portable format using industry standards;</li> <li>• Reduction methods are used, where necessary;</li> <li>• Secure disposal of information stored on magnetic and non-magnetic media that prevents potential recovery of the information;</li> <li>• <b>[Other: Vendor to complete]</b></li> </ul>

### Sensitive data

For transfers of sensitive data, also describe the safeguards implemented such as strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures etc.:

**[Vendor to insert description of safeguards for the transfer of sensitive data.]**

—

*ANNEX III***SWISS ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES**

1. If the Personal Data is protected by the Swiss Federal Act on Data Protection, then the parties agree that the Standard Contractual Clauses will be amended and adapted as follows as far as such data is concerned: (i) the law that applies will be Swiss law ; (ii) the place of jurisdiction shall be at the data subject's domicile in Switzerland; (iii) the term "member state" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 c. and (iv), the references to the GDPR should be understood as references to the Swiss DPA insofar as the data transfers are subject to the Swiss Federal Data Protection Act.
2. The Standard Contractual Clauses shall, until the entry into force of the revised Swiss Federal Act on Data Protection, also protect the data of legal entities.

## ANNEX IV

## UK ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

**Part 1: Tables**

Table 1: Parties

<b>Start date</b>	The date of this Agreement	
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties' details</b>	<p>Full legal name: The Procter &amp; Gamble Company</p> <p>Trading name (if different): <b>[Insert]</b></p> <p>Main address (if a company registered address): One Procter &amp; Gamble Plaza, Cincinnati, Ohio 45202, United States of America</p> <p>Official registration number (if any) (company number or similar identifier): <b>[Insert]</b></p>	<p>Full legal name: <b>[Insert]</b></p> <p>Trading name (if different): <b>[Insert]</b></p> <p>Main address (if a company registered address): <b>[Insert]</b></p> <p>Official registration number (if any) (company number or similar identifier): <b>[Insert]</b></p>
<b>Key Contact</b>	<p>Full Name (optional): <b>[Insert]</b></p> <p>Job Title: <b>[Insert]</b></p> <p>Contact details including email: <b>[Insert]</b></p>	<p>Full Name (optional): <b>[Insert]</b></p> <p>Job Title: <b>[Insert]</b></p> <p>Contact details including email: <b>[Insert]</b></p>
<b>Signature (if required for the purposes of Section 2)</b>		

Table 2: Selected SCCs, Modules and Selected Clauses

<b>Addendum EU SCCs</b>	<p><input checked="" type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:</p> <p>Date: The date of the Agreement</p>
-------------------------	---

		Reference (if any): <input type="text"/> Other identifier (if any): <input type="text"/> Or <input type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex IA: List of Parties: Annex IA of this Agreement

---

Annex IB: Description of Transfer: Annex IB of this Agreement

---

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Annex II of this Agreement

---

Annex III: List of Sub processors (Modules 2 and 3 only): N/A

---

Table 4: Ending this Addendum when the Approved Addendum Changes

<p><b>Ending this Addendum when the Approved Addendum changes</b></p>	Which Parties may end this Addendum as set out in Section 19: <input type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter <input type="checkbox"/> neither Party
---	--

## Part 2: Mandatory Clauses

### *Entering into this Addendum*

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

### *Interpretation of this Addendum*

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.

UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

### *Hierarchy*

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

### *Incorporation of and changes to the EU SCCs*

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
  - a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
  - b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
  - c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.



13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
  - a. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
  - b. In Clause 2, delete the words:
 

“and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679”;
  - c. Clause 6 (Description of the transfer(s)) is replaced with:
 

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;
  - d. Clause 8.7(i) of Module 1 is replaced with:
 

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
  - e. Clause 8.8(i) of Modules 2 and 3 is replaced with:
 

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”
  - f. References to “Regulation (EU) 2016/679”, “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 (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
  - g. References to Regulation (EU) 2018/1725 are removed;
  - h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
  - i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
  - j. Clause 13(a) and Part C of Annex I are not used;
  - k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
  - l. In Clause 16(e), subsection (i) is replaced with:
 

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;
  - m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

*Amendments to this Addendum*

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

- a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
- b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

- a. its direct costs of performing its obligations under the Addendum; and/or
- b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

*Annex V***SERBIA ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES**

If the Personal Data is protected by the Serbian Law on personal data protection, then the parties agree that the Standard Contractual Clauses will be amended and adapted as follows as far as such data is concerned: (i) the law that applies will be Serbian law (ii) the place of jurisdiction shall be at the data subject's domicile in Serbia; (iii) the term "member state" must not be interpreted in such a way as to exclude data subjects in Serbia from the possibility of suing for their rights in their place of habitual residence (Serbia) in accordance with Clause 18 c. and (iv), the references to the GDPR should be understood as references to the Serbian Law on personal data protection insofar as the data transfers are subject to the Serbian Law on personal data protection.

In addition, the PARTIES agree to amend the following provisions in Exhibit B to update them as follows:

1. The term "Applicable Data Protection Law" is amended as follows:

**"Applicable Data Protection Law"** means the EU General Data Protection Regulation ("GDPR"), the UK GDPR, Swiss data protection law and Serbian law on data protection, as amended or replaced from time to time.

2. The first paragraph in "ANNEX I" is amended as follows:

"By signing we also agree to be bound by the UK, Swiss and Serbian Addenda to the EU Commission Standard Contractual Clauses at Annex IV and V.

3. Section C of Annex I is amended as follows:

"COMPETENT SUPERVISORY AUTHORITY - Identify the competent supervisory authority/ies in accordance with Clause 13 "To the extent that the data transfer is governed by the GDPR, the supervisory authority of the EU Member State where the data exporter is established, as specified in Annex I. A and Schedule 1. To the extent that the data transfer is governed by the Swiss Federal Act on Data Protection, the Swiss FDPIC. To the extent that the data transfer is governed by the Serbian law on data protection, the Serbian Commissioner for information of public importance and personal data protection."

## SCHEDULE 1

### LIST OF DATA EXPORTERS

#### SUBSIDIARIES OF THE PROCTER & GAMBLE COMPANY

1837, LLC	Ohio	2462
Agile Pursuits Franchising, Inc.	Ohio	2216
Agile Pursuits, Inc.	Ohio	2141
Arbora & Ausonia, S.L.U.	Spain	0491
Braun (Shanghai) Co., Ltd.	China	2008
Braun GmbH	Germany	2313
Braun Oral-B Ireland Limited	Ireland	2253
Celtic Insurance Company, Inc.	Vermont	2258
Charlie Banana (USA), LLC	Delaware	2467
Corporativo Procter & Gamble, S. de R.L. de C.V.	Mexico	0714
Detergent Products B.V.	Netherlands	2284
Detergent Products Sarl	Switzerland	0431
Detergenti S.A.	Romania	0593
Fameccanica Data S.p.A.	Italy	0498
Fameccanica Indústria e Comércio Do Brasil LTDA.	Brazil	2201
Fameccanica Machinery (Shanghai) Co., Ltd.	China	0934
Fameccanica North America, Inc.	Delaware	
Fater Central Europe SRL	Romania	
Fater Eastern Europe LLC	Russia	2362
Fater Portugal Unipessoal Lda	Portugal	2347
Fater S.p.A.	Italy	0483
Fater Temizlik Urunleri Ltd STI	Turkey	
First Aid Beauty Limited	Delaware	2455
Fountain Square Music Publishing Co., Inc.	Ohio	0040
FPG Oleochemicals Sdn. Bhd.	Malaysia	0372
Gillette (China) Limited	China	2006
Gillette (Shanghai) Ltd.	China	0324
Gillette Australia Pty. Ltd.	Australia	0854
Gillette Commercial Operations North America	Massachusetts	0029
Gillette del Uruguay, S.A.	Uruguay	2032
Gillette Diversified Operations Pvt. Ltd.	India	0972
Gillette Dominicana, S.A.S.	Dominican Republic	0146
Gillette Egypt S.A.E.	Egypt	0139
Gillette Group UK Ltd	U.K.	0977
Gillette Holding Company LLC	Delaware	0178
Gillette Holding GmbH	Germany	0852
Gillette India Limited	India	0973
Gillette Industries Ltd.	U.K.	0855
Gillette International B.V.	Netherlands	0979
Gillette Latin America Holding B.V.	Netherlands	0982
Gillette Management, LLC	Delaware	0856
Gillette Pakistan Limited	Pakistan	0149
Gillette Poland International Sp. z.o.o.	Poland	2031
Gillette U.K. Limited	U.K.	0869
Grooming Ventures - FL LLC	Florida	

Grooming Ventures LLC	Delaware	
Hyginett KFT	Hungary	0344
iMFLUX Inc.	Delaware	2348
Industries Marocaines Modernes SA	Morocco	0380
Laboratoire Mediflor S.A.S.	France	2448
Laboratorios Vicks, S.L.U.	Spain	0918
Lamberts Healthcare Ltd.	U.K.	2453
Liberty Street Music Publishing Company, Inc.	Ohio	0156
Limited Liability Company 'Procter & Gamble Trading Ukraine'	Ukraine	2160
LLC "Procter & Gamble - Novomoskovsk"	Russia	0614
LLC "Procter & Gamble Distributorskaya Compania"	Russia	0316
LLC "Procter & and Gamble Ukraine"	Ukraine	0576
Marcvenca Inversiones, C.A.	Venezuela	0478
Modern Industries Company - Dammam	Saudi Arabia	0409
Modern Products Company - Jeddah	Saudi Arabia	0411
Nature's Best Health Products Ltd.	U.K.	2454
New Chapter Canada Inc.	Canada	2343
New Chapter, Inc.	Delaware	2342
Olay LLC	Puerto Rico	2159
Oral-B Laboratories	Delaware	0170
P&G Consumer Health Germany GmbH	Germany	2442
P&G Distribution East Africa Limited	Kenya	2062
P&G Distribution Morocco SAS	Morocco	0140
P&G Hair Care Holding, Inc.	Delaware	0066
P&G Health Austria GmbH & Co. OG	Austria	2452
P&G Health France S.A.S.	France	2447
P&G Health Germany GmbH	Germany	2443
P&G Healthcare (Zhejiang) Limited	China	2369
P&G Industrial Peru S.R.L.	Peru	0785
P&G Innovation Godo Kaisha	Japan	2205
P&G Investment Management Ltd.	United Arab Emirates	2458
P&G Israel M.D.O. Ltd.	Israel	0872
P&G Japan G.K.	Japan	2039
P&G K.K.	Japan	0822
P&G Northeast Asia Pte. Ltd.	Singapore	0820
P&G Prestige Godo Kaisha	Japan	0366
P&G South African Trading (Pty.) Ltd.	South Africa	0134
Petersburg Products International LLC	Russia	2021
PG13 Launchpad Alpha, Inc.	Delaware	2461
PG13 Launchpad Beta, Inc.	Delaware	2463
PG13 Launchpad Gamma, Inc.	Delaware	2472
PGT Healthcare LLP	Delaware	2289
Phase II Holdings Corporation	Philippines	
Procter & Gamble (Chengdu) Ltd.	China	0581
Procter & Gamble (China) Ltd.	China	0584
Procter & Gamble (China) Sales Co., Ltd.	China	2294
Procter & Gamble (Egypt) Manufacturing Company	Egypt	0484
Procter & Gamble (Guangzhou) Consumer Products Co., Ltd.	China	2338
Procter & Gamble (Guangzhou) Enterprise Management Service Company Limited	China	2370
Procter & Gamble (Guangzhou) Ltd.	China	0293
Procter & Gamble (Guangzhou) Technology Innovation Co., LTD.	China	2437

Procter & Gamble (Health & Beauty Care) Limited	U.K.	0456
Procter & Gamble (Jiangsu) Ltd.	China	2273
Procter & Gamble (L&CP) Limited	U.K.	0688
Procter & Gamble (Malaysia) Sdn Bhd	Malaysia	0373
Procter & Gamble (Manufacturing) Ireland Limited	Ireland	0352
Procter & Gamble (Singapore) Pte. Ltd.	Singapore	0412
Procter & Gamble Algeria EURL	Algeria	0870
Procter & Gamble Amazon Holding B.V.	Netherlands	2050
Procter & Gamble Amiens S.A.S.	France	0579
Procter & Gamble Argentina SRL	Argentina	0501
Procter & Gamble Asia Pte. Ltd.	Philippines	2286
Procter & Gamble Australia Proprietary Limited	Australia	0255
Procter & Gamble Azerbaijan Services LLC	Azerbaijan	0289
Procter & Gamble Bangladesh Private Ltd.	Bangladesh	0649
Procter & Gamble Blois S.A.S.	France	0730
Procter & Gamble Brazil Holdings B.V.	Netherlands	0987
Procter & Gamble Bulgaria EOOD	Bulgaria	0600
Procter & Gamble Business Services Canada Company	Canada	0836
Procter & Gamble Canada Holding B.V.	Netherlands	0919
Procter & Gamble Chile Limitada	Chile	0536
Procter & Gamble Colombia Ltda.	Colombia	0295
Procter & Gamble Commercial de Cuba, S.A.	Cuba	0298
Procter & Gamble Commercial LLC	Puerto Rico	2053
Procter & Gamble Czech Republic s.r.o.	Czech Republic	0903
Procter & Gamble d.o.o. za trgovinu	Croatia	0751
Procter & Gamble Danmark ApS	Denmark	0736
Procter & Gamble de Venezuela, S.C.A.	Venezuela	2167
Procter & Gamble de Venezuela, S.R.L.	Venezuela	2168
Procter & Gamble Detergent (Beijing) Ltd.	China	0582
Procter & Gamble Deutschland GmbH	Germany	2225
Procter & Gamble Distributing (Philippines) Inc.	Philippines	0829
Procter & Gamble Distributing New Zealand Limited	New Zealand	0392
Procter & Gamble Distribution Company (Europe) BV	Belgium	0511
Procter & Gamble Distribution S.R.L.	Romania	0943
Procter & Gamble do Brasil Ltda.	Brazil	0273
Procter & Gamble do Brazil, LLC	Delaware	0056
Procter & Gamble do Nordeste S/A	Brazil	0272
Procter & Gamble doo Beograd	Serbia and Montenegro	0605
Procter & Gamble DS Polska Sp. z o.o.	Poland	2030
Procter & Gamble Eastern Europe, LLC	Ohio	0083
Procter & Gamble Ecuador Cia. Ltda.	Ecuador	0585
Procter & Gamble Egypt	Egypt	0302
Procter & Gamble Egypt Distribution	Egypt	2148
Procter & Gamble Egypt Holding	Egypt	2147
Procter & Gamble Egypt Supplies	Egypt	2149
Procter & Gamble Energy Company LLC	Ohio	
Procter & Gamble España, S.A.U.	Spain	0747
Procter & Gamble Europe SA	Switzerland	0700
Procter & Gamble Far East, Inc.	Ohio	0051
Procter & Gamble Finance (U.K.) Ltd.	U.K.	0930
Procter & Gamble Finance Holding Ltd.	U.K.	2428

Procter & Gamble Finance Management S.a.r.l.	Luxembourg	2357
Procter & Gamble Financial Investments LLP	U.K.	2427
Procter & Gamble Financial Services Ltd.	U.K.	0602
Procter & Gamble Finland OY	Finland	0737
Procter & Gamble France S.A.S.	France	0577
Procter & Gamble Germany GmbH	Germany	0917
Procter & Gamble Germany GmbH & Co. Operations oHG	Germany	0901
Procter & Gamble Ghana Trading Limited	Ghana	2374
Procter & Gamble GmbH	Germany	0335
Procter & Gamble Grundstücks-und Vermögensverwaltungs GmbH & Co. KG	Germany	2157
Procter & Gamble Gulf FZE	United Arab Emirates	0799
Procter & Gamble Hair Care, LLC	Delaware	0094
Procter & Gamble Health Belgium BV	Belgium	2446
Procter & Gamble Health Limited	India	2449
Procter & Gamble Health Ltd.	U.K.	2445
Procter & Gamble Health Poland Sp. z o.o.	Poland	0978
Procter & Gamble Hellas Single Member Ltd.	Greece	0338
Procter & Gamble Holding (Thailand) Limited	Thailand	0837
Procter & Gamble Holding France S.A.S.	France	0310
Procter & Gamble Holding GmbH	Germany	0330
Procter & Gamble Holding S.r.l.	Italy	0802
Procter & Gamble Holdings (UK) Ltd.	U.K.	0927
Procter & Gamble Home Products Private Limited	India	0572
Procter & Gamble Honduras S de RL	Honduras	2465
Procter & Gamble Hong Kong Limited	Hong Kong	0342
Procter & Gamble Hungary Wholesale Trading Partnership (KKT)	Hungary	0345
Procter & Gamble Hygiene & Health Care Limited	India	0348
Procter & Gamble Inc.	Canada	0283
Procter & Gamble India Holdings, Inc.	Ohio	0095
Procter & Gamble Indochina Company Limited	Vietnam	0693
Procter & Gamble Industrial - 2012 C.A.	Venezuela	2351
Procter & Gamble Industrial e Comercial Ltda.	Brazil	0682
Procter & Gamble Industrial S.C.A.	Venezuela	2162
Procter & Gamble Interamericas de Costa Rica, Limitada	Costa Rica	0656
Procter & Gamble Interamericas de El Salvador, Limitada de Capital Variable	El Salvador	0719
Procter & Gamble Interamericas de Guatemala, Limitada	Guatemala	0718
Procter & Gamble Interamericas de Panama, S. de R.L.	Panama	0396
Procter & Gamble International Operations Pte Ltd	Singapore	2282
Procter & Gamble International Operations SA	Switzerland	0800
Procter & Gamble International Operations SA-ROHQ	Philippines	0753
Procter & Gamble International Sarl	Switzerland	0896
Procter & Gamble Investment Company (UK) Ltd.	U.K.	0928
Procter & Gamble Investment Holding B.V.	Netherlands	2441
Procter & Gamble Italia, S.p.A.	Italy	0357
Procter & Gamble Kazakhstan Distribution LLP	Kazakhstan	2432
Procter & Gamble Korea S&D Co.	Korea	0823
Procter & Gamble Korea, Inc.	Korea	0493
Procter & Gamble Leasing LLC	Ohio	0046
Procter & Gamble Levant S.A.L.	Lebanon	0370
Procter & Gamble Limited	U.K.	0455
Procter & Gamble LLC	Russia	0474

Procter & Gamble Manufacturing (Thailand) Limited	Thailand	0440
Procter & Gamble Manufacturing (Tianjin) Co. Ltd.	China	0676
Procter & Gamble Manufacturing Belgium N.V.	Belgium	0685
Procter & Gamble Manufacturing Berlin GmbH	Germany	2066
Procter & Gamble Manufacturing GmbH	Germany	0613
Procter & Gamble Manufacturing Mexico S. de R.L. de C.V.	Mexico	2373
Procter & Gamble Manufacturing SA (Pty) Ltd	South Africa	2171
Procter & Gamble Marketing Latvia Ltd.	Latvia	0648
Procter & Gamble Marketing Romania SRL	Romania	0575
Procter & Gamble Mataro, S.L.U.	Spain	0423
Procter & Gamble Mexico Holding B.V.	Netherlands	0761
Procter & Gamble Mexico Inc.	Delaware	2393
Procter & Gamble Middle East FZE	United Arab Emirates	2368
Procter & Gamble Nederland B.V.	Netherlands	0505
Procter & Gamble Netherlands Services B.V.	Netherlands	0899
Procter & Gamble Nigeria Limited	Nigeria	0485
Procter & Gamble Norge AS	Norway	0611
Procter & Gamble Operations Polska Sp. z o.o.	Poland	0533
Procter & Gamble Overseas India B.V.	Netherlands	2064
Procter & Gamble Overseas Ltd.	U.K.	0929
Procter & Gamble Pakistan (Private) Limited	Pakistan	0394
Procter & Gamble Peru S.R.L.	Peru	0398
Procter & Gamble Philippines Business Services Inc.	Philippines	2474
Procter & Gamble Philippines, Inc.	Philippines	0403
Procter & Gamble Polska Sp. z o.o	Poland	0404
Procter & Gamble Portugal - Produtos De Consumo, Higiene e Saúde S.A.	Portugal	0570
Procter & Gamble Product Supply (U.K.) Limited	U.K.	0661
Procter & Gamble Productions, Inc.	Ohio	0004
Procter & Gamble Productos de Consumo, S.L.U.	Spain	2310
Procter & Gamble Retail Services Sarl	Switzerland	2435
Procter & Gamble RHD, Inc.	Ohio	0018
Procter & Gamble RSC Regional Service Company Ltd.	Hungary	0908
Procter & Gamble S.r.l.	Italy	0591
Procter & Gamble Service, GmbH	Germany	0640
Procter & Gamble Services (Switzerland) SA	Switzerland	0752
Procter & Gamble Services Company N.V.	Belgium	0270
Procter & Gamble Services LLC	Russia	0779
Procter & Gamble Sverige AB	Sweden	0118
Procter & Gamble Switzerland SARL	Switzerland	0430
Procter & Gamble Taiwan Limited	Taiwan	0438
Procter & Gamble Taiwan Sales Company Limited	Taiwan	2355
Procter & Gamble Technical Centres Limited	U.K.	0687
Procter & Gamble Technology (Beijing) Co., Ltd.	China	0692
Procter & Gamble Trading (Thailand) Limited	Thailand	0441
Procter & Gamble Tuketim Mallari Sanayii A.S.	Turkey	0444
Procter & Gamble UK	U.K.	0686
Procter & Gamble UK Group Holdings Ltd	U.K.	2211
Procter & Gamble UK Parent Company Ltd.	U.K.	2287
Procter & Gamble Universal Holding B.V.	Netherlands	2344
Procter & Gamble Vietnam Company Limited	Vietnam	0609
Procter & Gamble West Africa Sarl	Switzerland	2358



Procter & Gamble, Spol. s.r.o. (Ltd.)	Slovak Republic	0556
Procter & Gamble-Rakona s.r.o.	Czech Republic	0300
Procter and Gamble Lanka (Private) Limited	Sri Lanka	0662
Progam Realty & Development Corporation	Philippines	0601
PT Procter & Gamble Home Products Indonesia	Indonesia	0604
PT Procter & Gamble Operations Indonesia	Indonesia	2280
Redmond Products, Inc.	Minnesota	
Richardson-Vicks Real Estate Inc.	Ohio	0068
Riverfront Music Publishing Co., Inc.	Ohio	0041
Rosemount LLC	Delaware	0057
Series Acquisition B.V.	Netherlands	0143
Seven Seas Limited	U.K.	2444
Shulton, Inc.	New Jersey	0012
Snowberry New Zealand Limited	New Zealand	2439
SPD Development Company Limited	U.K.	2156
SPD Swiss Precision Diagnostics GmbH	Switzerland	2151
Sunflower Distributing LLC	Delaware	
Tambrands Inc.	Delaware	0089
TAOS - FL, LLC	Florida	
Temple Trees Impex & Investment Private Limited	India	0659
The Dover Wipes Company	Ohio	0065
The Gillette Company LLC	Delaware	0069
The Procter & Gamble Distributing LLC	Delaware	0003
The Procter & Gamble Global Finance Company, LLC	Ohio	0020
The Procter & Gamble Manufacturing Company	Ohio	0002
The Procter & Gamble Paper Products Company	Ohio	0007
The Procter & Gamble U.S. Business Services Company	Ohio	0005
This is L. Inc.	Delaware	2457
US CD LLC	Delaware	2152
Vidal Sassoon (Shanghai) Academy	China	0798
VitaminHaus Pty Ltd	Australia	2477
VitaminHaus Pty Ltd	U.K.	2478
Walker & Co. Brands, Inc.	Delaware	2456
Winc Design Limited	Hong Kong	2466
Zenlen, Inc.	Delaware	2438

**SCHEDULE 2**

**LIST OF DATA IMPORTERS (Data importer to include if applicable)**