**DATA PROCESSING AGREEMENT**

This Data Processing Agreement (“**DPA**”) is entered into on the dates below written, and effective \_\_\_\_\_\_\_\_ 2020 (“**Effective Date**”), by and between International Flavors & Fragrances, Inc., [address][on its own behalf and on behalf of its subsidiaries and affiliates (“**Customer**”) and [name of third party], [address](“**Third Party**”) (each a “**Party**” and together the “**Parties**”).

WHEREAS, the Parties have entered into a [services agreement (the “**Service Agreement**”)] whereby Third Party provides Services (as defined in the Service Agreement) to Customer;

WHEREAS, in connection with the Services, Third Party processes, on Customer’s behalf, personal data the processing of which is subject to specific obligations under applicable data protection laws;

WHEREAS, Customer requires Third Party to agree to process such personal data in accordance with the requirements of applicable data protection laws;

NOW THEREFORE, for good and valuable consideration, the adequacy and sufficiency of which hereby are acknowledged, the Parties agree as follows.

1. Definitions
	1. "**Data Protection Law**" shall mean all applicable data privacy and data protection laws including, but not limited to, (i) the EU General Data Protection Regulation (Regulation 2016/679) ("**GDPR**") and any implementing or supplementing law; (ii) the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Addendums etc.) (EU Exit) Regulations 2019, together with the Data Protection Act 2018, the Data Protection, Privacy and Electronic Communications (Addendums etc.) (EU Exit) Regulations 2019 (“**UK** **GDPR**”); (iii) the Swiss Federal Act on Data Protection (“**Swiss Act**”); and (iv) the California Consumer Privacy Act of 2018; each as may be amended from time to time and to the extent applicable to (as the case may be) to Processing carried out by Third Party pursuant to this DPA.
	2. “**Personal Data**” means personal data that is Processed by Third Party on behalf of Customer in connection with the provision of the Services and that is subject to Data Protection Law.
	3. “**Personal Data Breach**” means a suspected or actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed when that Personal Data is in the possession or under control of Third Party or its agents or subcontractors;
	4. “**SCCs**” means (i) the standard contractual clauses for Processors approved by the European Commission pursuant to Decision C (2010)593; or (ii) any other contractual terms that are valid under Data Protection Law to effect transfers of Personal Data; in each case as they may be amended or replaced from time to time by the European Commission, or by any other data protection authority with jurisdiction.
	5. “**Special Categories of Personal Data**” means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, sex life, or sexual orientation, genetic data and biometric data when Processed for the purpose of uniquely identifying a natural person and information about criminal history, or as otherwise defined by Data Protection Law.
	6. “**Sub-processor**” means an entity that Processes Personal Data at the request of Third Party.
	7. “**Controller**”, “**Data Subject**”, “**personal data**”, “**Processing**”, “**Processor**” and “**Supervisory Authority**” have the same meanings as defined in Data Protection Law and corresponding cognate terms shall be interpreted accordingly.
2. Scope of Personal Data and Processing
	1. *Scope of Personal Data*. This DPA shall apply to all transfers of Personal Data from Customer to the Third Party and to the processing of Personal Data by the Third Party.
	2. *Processing of Personal Data*. When Processing Personal Data, Third Party acts as Processor and Customer acts as Controller. Third Party agrees to Process Personal Data solely for the duration set forth in and subject to this DPA, in accordance with **Attachment 1**, which describes (notably) the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects.
	3. *Compliance with Laws*. Third Party will Process Personal Data in compliance with the terms of the Services Agreement, this DPA and Third Party’s obligations under applicable law.
3. Third Party Obligations for Processing
	1. *Instructions.* Third Party shall only Process Personal Data for the purpose of Third Party’s providing the Services to Customer in accordance with Customer’s documented instructions, unless required to otherwise Process Personal Data under Data Protection Law, as applicable, in which case Third Party shall inform Customer, unless the relevant law prohibits such information on important grounds of public interest. Third Party shall inform Customer immediately if in Third Party’s opinion an instruction infringes Data Protection Law.
	2. *Limitations on Processing*. Without limiting the generality of Section 3.1, Third Party shall not retain, use, or disclose Personal Data: (1) for any purpose (including, but not limited to, any commercial purpose) other than to perform the Services for Customer or (2) outside of the direct business relationship between Customer and Third Party. Third Party shall not sell, rent, release, disclose, disseminate, make available, transfer or otherwise communicate Personal Data to any third party for monetary or other valuable consideration.
	3. *Confidentiality of Personal Data*. Third Party will maintain the confidentiality of all Personal Data Processed. Third Party represents that it has required all of its employees or other personnel (including independent contractors and subcontractors) that will Process Personal Data to sign a confidentiality agreement prohibiting the disclosure of Personal Data Processed except as permitted by this DPA or as required by law.
	4. *Audits*. Third Party shall promptly, after written request from Customer, make available to Customer all information necessary to demonstrate Customer’s compliance with the obligations set forth in this DPA and Data Protection Law. Third Party will permit Customer, directly or through a contractor in possession of the required professional qualifications and bound by a duty of confidentiality, to conduct site audits of the information technology and information security controls for all facilities used to Process Personal Data.
	5. *Impact Assessments*. Third Party shall promptly provide information requested by Customer to assist Customer in conducting a data protection impact assessment or consulting a Supervisory Authority in respect of the Personal Data.
	6. *Requests from Data Subjects.* Third Party shall assist Customer in complying with its obligations under Data Protection Law to respond to Data Subject requests by carrying out any such request within five (5) business days of receiving a written request from Customer. Third Party will immediately forward to Customer with any requests from Data Subjects concerning Personal Data that are sent directly to Third Party and shall not respond thereto unless instructed by Customer.
4. Third Party Security Obligations
	1. *Security Measures*. Third Party shall maintain a comprehensive written information privacy and security program that includes the measures set forth in **Appendix 2 to** **Attachment 2**, including technical, physical, and organizational safeguards 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 natural persons, in order to protect against reasonably foreseeable risks to the security, confidentiality, integrity and resilience of Personal Data, which risks could result in the unauthorized disclosure, use, alteration, destruction or other compromise of the Personal Data, including a Personal Data Breach.
	2. *Encryption or Redaction.* Third Party shall at all times, both at rest and in transit, encrypt, redact or de-identify by irreversibly removing individual names, all Special Personal Information that Third Party receives from Customer or has access to in connection with the Processing of Personal Data. “**Special Personal Information**” means an individual’s first name or first initial and the individual’s last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

#### Social security number.

#### Driver’s license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

#### Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

#### Any individually identifiable information, in electronic or physical form, regarding the individual’s medical history or medical treatment or diagnosis by a health care professional.

#### An individual’s insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.

#### Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

#### A username or email address in combination with a password or security question and answer that would permit access to a California resident’s electronic mail account.

“Special Personal Information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

* 1. *Reporting Personal Data Breaches*. Third Party will maintain (and, if necessary, develop and implement) a written response plan to ensure that any Personal Data Breach implicating Personal Data will be promptly discovered by Third Party and promptly reported to Customer. Third Party shall report to Customer in writing within 48 hours any Personal Data Breach implicating Personal Data of which Third Party becomes aware, regardless of whether the Personal Data Breach results from the actions of Third Party or its agents or Sub-processors. Third Party shall provide the following information as and when available: (1) a description of the Personal Data Breach; (2) the date that the Personal Data Breach occurred; (3) the date and time at which the Third Party became aware of the Personal Data Breach; (4) the affected categories of Personal Data, including Special Categories of Personal Data, if any, for each affected Data Subject; (5) the approximate number of Data Subjects affected and the approximate number of records containing Personal Data; (6) a description of the steps taken to mitigate the Personal Data Breach and prevent recurrence; (7) the likely consequences of the Personal Data Breach; and (8) all other information reasonably requested by Customer in order to comply with its obligations under applicable law or contracts.
	2. *Notifications*. Third Party shall not notify any third party of any Personal Data Breach implicating Personal Data without Customer’s prior written authorization.
	3. *Mitigation of Damages by Third Party and Cooperation*. Third Party agrees to take, at its own expense, measures reasonably necessary to mitigate any harmful effect of a Personal Data Breach implicating Personal Data, and shall cooperate, at its own expense, with Customer in its investigation and remediation of any such Personal Data Breach. Third Party will promptly reimburse Customer for all imputed and out-of-pocket costs reasonably incurred by Customer in connection with the Personal Data Breach, including, but not limited to, costs related to Customer’s provision of notices to any Supervisory Authority or affected Data Subjects and to any services offered to affected Data Subjects.
1. Sub-processors
	1. *Consent to Processing by Sub-Processors*. Third Party will not engage any Sub-processor to Process Personal Data unless: (i) Customer has provided its prior written consent; and (ii) Third Party formally appoints in writing such Sub-processor to Process the Personal Data and imposes via a binding contract or other legal act containing the same data protection terms as this DPA. Third Party shall remain responsible and liable to Customer for the acts and omissions of any Sub-processor with regard to Personal Data Processed by the Sub-processor. Subject to the foregoing, Customer consents to Third Party’s disclosure of Personal Data to the Sub-processors identified in **Attachment 3**. Third Party must notify Customer in writing at least thirty (30) days prior to appointing or replacing a Sub-processor identified in **Attachment 3**, and Customer may object to such appointment or replacement, in which case Third Party will either not appoint or replace the Sub-processor to Process Personal Data or, if this is not possible, Customer may elect to suspend or terminate the Service Agreement without penalty, indemnity or damages of any nature whatsoever.
	2. *Sub-processor Security Measures*: Third Party shall obtain reasonable assurances, in writing, from any Sub-processor to whom Third Party discloses Personal Data that the Sub-processor (1) will implement reasonable and appropriate physical, technical and organizational safeguards to protect Personal Data in compliance with this DPA and Data Protection Law, including the restrictions on data transfers, as applicable; and (2) will notify Third Party within 24 hours of becoming aware of any Personal Data Breach.
2. Data Transfers
	1. *Data Transfers by Vendor.* Vendor will not transfer Personal Data outside the EEA, the United Kingdom or Switzerland unless (1) Customer has provided prior written permission for the transfer, and (2) in addition to the other requirements set forth in this Addendum, Vendor documents and ensures an adequate level of protection for such transfer in accordance with Data Protection Law.
	2. *Standard Contractual Clauses.* Customer (and any Customer affiliate, as the case may be), as data exporter, and Third Party, as a data importer, hereby execute, *mutatis mutandis* as the case may be, the SCCs, which are expressly incorporated herein by reference and shall apply to the Personal Data and take effect as from the commencement of a transfer of Personal Data by Customer (or any Customer affiliate, as the case may be)to Third Party, to the extent such transfer would be prohibited by Data Protection Law in the absence of the SCCs.
	3. *Third Party Inter-company Agreements.* Third Party will provide a copy of any inter-company agreements incorporating SCCs or similar transfer terms to Customer upon Customer’s written request, subject to redaction as may be appropriate.
3. Termination
	1. *Return or Destruction of Personal Data*. Within thirty (30) business days of the termination of the Service Agreement, Third Party, at Customer’s election but at Third Party’s expense, shall return, destroy, and/or transfer to a third party designated in writing by Customer, all Personal Data. If Customer directs Third Party to destroy the Personal Data, Third Party shall do so in a secure and irreversible manner. Within five (5) business days of the date of destruction, Third Party will provide Customer with a written certification, signed by an authorized representative, representing that the Personal Data has been permanently and securely destroyed and describing the method of destruction.
	2. *Third Party’s Retention of Personal Data*. If, at the termination of the Service Agreement, Third Party delivers to Customer written notice explaining that applicable law requires Third Party to retain the Personal Data, and Customer is satisfied that Third Party must retain the Personal Data, then Customer may excuse Third Party from complying, in whole or in part, Section 7.1 above. In this case, Third Party shall (1) deliver to Customer, at Third Party’s expense, within fifteen (15) business days of the termination of the Service Agreement, a duplicate of all Personal Data retained by Third Party, and (2) the requirements of this DPA shall continue to apply to the retained Personal Data for as long as Third Party maintains the Personal Data.
4. Miscellaneous
	1. *Indemnification*. Third Party shall defend and indemnify Customer, its parent and subsidiary corporations, officers, directors, employees and agents (“**Indemnified Parties**”) for any and all claims, inquiries, investigations, losses, costs, reasonable attorneys’ fees, penalties, damages and, to the extent permissible by law, all civil and criminal liabilities, incurred by any Indemnified Party resulting from (1) any Processing of Personal Data not permitted by the Services Agreement, this DPA or Data Protection Law, (2) any Personal Data Breach implicating Personal Data in the possession, custody or control of Third Party or any of its agents or Sub-processors, or (3) any other breach of this DPA or Data Protection Law by Third Party.
	2. *Effect of DPA*. This DPA amends the Service Agreement, and all other existing agreements between Customer and Third Party relating to Third Party’s Processing of personal data on behalf of Customer (“**Other Agreements**”), and supersedes any inconsistent provisions in the Service Agreement or Other Agreements to the extent they apply to Personal Data. In the event of any conflict between the terms of this DPA on the one hand, and the Service or Other Agreements on the other hand, the terms of this DPA shall prevail. All other terms and conditions in the Service Agreement and Other Agreements shall remain in full force and effect.
	3. *Amendment*. The Parties agree to amend this DPA and/or the Service Agreement from time to time as may be necessary to permit Customer to remain in compliance with Data Protection Law and any other applicable law.
	4. *Survival.* Third Party’s obligations and duties under this DPA with respect to Personal Data shall survive the termination of the Service Agreement and of this DPA and shall continue for as long as the Personal Data remains in the possession or under control of Third Party or of its agents or Sub-processors.
5. Certification

By executing this DPA, Third Party certifies that it understands the restrictions on its Processing of Personal Data set forth in this DPA, and agrees that it will comply with them.

|  |  |
| --- | --- |
| **[IFF]**By:                                                             Name:                                                        Title:                                                            Date:                                              , 2020 | **[NAME OF VENDOR]** By:                                                             Name:                                                        Title:                                                           Date:                                              , 2020 |

**ATTACHMENT 1 TO DATA PROCESSING ADDENDUM**

**Subject matter and Nature of Processing by Third Party:**

***To be completed***

**Purposes of Processing by Third Party:**

***To be completed***

**Categories of Data Subjects Whose Personal Data Is Processed by Third Party:**

***To be completed***

**Categories of Personal Data Processed by Third Party:**

***To be completed***

**Categories of Sensitive Data Processed by Third Party:**

***To be completed***

**ATTACHMENT 2 TO DATA PROCESSING ADDENDUM**

**Commission Decision C(2010)593
Standard Contractual Clauses (processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel.:

e-mail:

Other information needed to identify the organisation: N/A

 (the data **exporter**)

And

Name of the data importing organisation:

Address:

Tel.:

e-mail:

Other information needed to identify the organisation: N/A

 (the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

**Definitions**

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[[1]](#footnote-1);

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law****'*** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

**Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

**Third-party beneficiary clause**

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

**Obligations of the data exporter**

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

**Obligations of the data importer**

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

**Liability**

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

**Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

**Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

**Governing Law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

**Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

**Subprocessing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely the United Kingdom.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

**Obligation after the termination of personal data processing services**

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**On behalf of the data exporter:**

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature………………………………………. Date ……………………………………….

**On behalf of the data importer:**

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature………………………………………. Date ……………………………………….

 (stamp of organisation)

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

**Data exporter**

The data exporter is (please specify briefly your activities relevant to the transfer):

**Data importer**

The data importer is (please specify briefly activities relevant to the transfer):

**Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

**Categories of data**

The personal data transferred concern the following categories of data (please specify):

**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify):

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

DATA EXPORTER

Name: ……………………

Authorised Signature ……………………

DATA IMPORTER

Name:………………………………

Authorised Signature ……………………

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

***To be completed***

attachment 3 to the data processing addendum

Customer agrees to Third Party’s use of the following Sub-processors to Process Personal Data, subject to the terms of the DPA:

|  |  |  |
| --- | --- | --- |
| **Sub-processor’s Name** | **Sub-processor’s Address** | **Description Of Sub-processing Services** |
| ***To be completed*** |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone. [↑](#footnote-ref-1)